卡巴斯基實驗室

Kaspersky® Internet Security 2009

使用者手冊

KASPERSKY® INTERNET SECURITY 2009

使用者手冊

卡巴斯基實驗室
香港區獨家總代理
立高科技有限公司
http://www.kaspersky.com.hk

親愛的 Kaspersky Internet Security 2009 的使用者！

感謝您選擇我們的產品。我們希望該檔檔在您使用過程中能夠為您提供幫助，並為您解答產品相關的疑問。

電話(Tel) ：(852)36934668

傳真(Fax)：(852)36934778

http://www.kaspersky.com.hk/

http://www.kaspersky.com.hk/support/

目 錄

引言

產品描述

您可以從我們的銷售商處購買盒裝產品，或在網上購買產品。 如果您購買了盒裝產品，將獲得以下內容：

- 安裝光碟（包含安裝程式檔和 PDF 文檔）。
- 快速安裝指南。
- 產品啟動碼。

最終用戶授權授權合約是您與卡巴斯基實驗室的有效法定協定，表明了您使用所購產品時需要遵守的條款。

請仔細閱讀最終用戶授權授權合約！

註冊使用者服務

卡巴斯基實驗室為所有合法的註冊使用者提供額外的服務，提高應用程式性能。 在購買授權許可之後，您就成為一個註冊用戶，在授權許可有效期內，您將享受以下服務：

- 每小時都在更新的應用程式資料庫和套裝軟體更新；
- 您可以通過電話或郵件獲得關於安裝，設定和使用產品的技術支援；
-

我們不提供關於作業系統的性能和使用，以及或其它非卡巴斯基的技術支援。

硬體和軟體需求

想要確保程式具備正常的功能，電腦必須具備如下最小的系統需求：

基本需求：

- 300 MB 可用的磁碟空間；
- CD-ROM (從 CD 安裝 Kaspersky Internet Security 2009)；
- Microsoft Internet Explorer 6.0 或更高 (更新應用程式資料庫和軟體模組)；
- Microsoft Windows Installer 2.0。

4 *Microsoft Windows XP Home Edition (Service Pack 2)*， Microsoft Windows XP Professional (Service Pack 2)， Microsoft Windows XP Professional x64 Edition：

- Intel Pentium 300 MHz 處理器或更高；
- 256 MB 可用記憶體。

4 *Microsoft Windows Vista Home Basic*； *Microsoft Windows Vista Home Premium*；*Microsoft Windows Vista Business*；*Microsoft Windows Vista Enterprise*；*Microsoft Windows Vista Ultimate*：

- Intel Pentium 800 MHz 32位(x86) / 64位(x64) 處理器或更高；
- 512 MB 剩餘記憶體。

Kaspersky Internet Security 2009

Kaspersky Internet Security 2009 是新一代的資訊保護方案。

Kaspersky Internet Security 2009 與其它軟體並和以往的同類卡巴斯基實驗室的產品真正區別的是，它能為使用者電腦上的資料安全提供多面性的保護。

獲得程式的資訊

如果您有任何關於購買，安裝或使用 Kaspersky Internet Security 的問題，我們很樂意為您解答。

卡巴斯基實驗室提供各種應用程式的資訊資源。您可以根據問題的重要性和緊急狀況，選擇最合適的。

幫助資源

您可以參考應用程式的以下資訊來源：

- 卡巴斯基實驗室網站上的應用程式頁面；
- 技術支援網站 (在知識庫)；
- 快速支援服務；
- 說明文件。

卡巴斯基實驗室網站上的應用程式頁面

http://www.kaspersky.com.hk/KL-Products/homeuser/

該頁面提供了程式的常規資訊，以及它的功能和選項的常規資訊。

技術支援網站的應用程式頁面(知識庫) .

http://www.kaspersky.com.k/support/

在該頁面，您會找到技術支援文章。

這些文章包含購買、安裝和應用程式使用方面的有用資訊建議和常見問題問答。例如，在個人用戶中，管理授權，設定資料庫更新，或啟動程式失敗。這些文章都提供了問題的解決方法，不僅僅是本產品的，還有其它產品。

快速支援服務

在該標籤，您可以找到定期更新的一些常見問題答案。如要使用該服務，您需要連接互聯網。 在主應用程式視窗，點擊技術支援的連結，在打開的視窗中點擊快速支援按鈕。

說明文件

Kaspersky Internet Security 的安裝包裡有用戶手冊(PDF格式)。該說明檔含有應用程式功能的描述。

聯繫銷售部門

如果您在選擇、購買產品或需要延長產品的使用方面有疑問，請致電我們的銷售部門：

(852) 3693 4668

或是通過電子郵件發送您的問題至：info@kaspersky.com.hk。

聯繫技術支援服務

如果您已經購買了該產品，那麼您就可以通過電話或網路的方式從技術支援服務獲取您想知道的資訊。

卡巴斯基實驗室的技術支援服務專家將會就您提出的關於程式的安裝、使用，以及如果您的電腦被病毒感染等問題，給出有用的建議以解決這些問題。

在聯繫技術支援之前，請閱讀卡巴斯基實驗室產品的技術支援規則。

通過電話支援

如果您有緊急事件，請撥打本地的技術支援服務電話。在您給技術支援專家打電話之前，請收集您電腦和反病毒程式的資訊。這將有助於我們的專家更快速的幫助您。

卡巴斯基官方論壇

如果您不需要立即得到問題的答案，可以在我們的官方論壇上 http://forum.kaspersky.com/ 提出問題，跟我們的工作人員或其它用戶一起討論。

在這個論壇上，您可以查看已有的帖子，留下您的評論和看法，發表新的帖子，或搜索帖子。

Kaspersky Internet Security 2009 的新功能

Kaspersky Internet Security 2009 是全面的資料保護工具。對所有通道的資料傳輸和交換提供多方位的保護。為每個模組提供了靈活的設定，能滿足不同使用者對卡巴斯基反病毒的不同要求。

讓我們仔細討論下 Kaspersky Internet Security 2009 的新功能：

新功能：

- 應用程式控制模組，該模組跟免疫防護和防火牆一起全面防禦各種威脅。應用程式控制模組可以將作業系統的程式分為不同等級，如受信任，高限制等。不同級別的應用程式如要訪問個人隱私資料和作業系統檔案時具有不同許可權，如有的可以讀取，有的可以修改，這樣可以防止應用程式執行危險的操作。
- 即時通訊防護，為即時通訊程式提供保護。該模組掃描接收和發送的資訊中是否包含惡意物件。
- 在安全的虛擬環境運行不知名的程式 - 在沙箱防護運行。這樣可以在一個虛擬的環境中運行應用程式，可以更好的保證系統安全。
- 網頁防護。該模組檢查網頁連結是否屬於可疑網站和釣魚網站列表。該模組換入在Microsoft Internet Explorer 和 Mozilla Firefox 瀏覽器中作為外掛程式。
- 監控訪問釣魚網站，當檢測到訪問網站的動作時，通過使用釣魚網址的資料庫，掃描郵件資訊和網頁中的連結來防禦釣魚攻擊。您可以檢查網站位址是否包含在釣魚網站位址清單中；該項僅適用於網頁防護，即時通訊防護和垃圾郵件防護。
- 弱點掃描；它令檢測和消除在作業系統和電腦上的應用程式的安全威脅以及安裝弱點變得容易。

新介面：

- 保護中心。將保護使用者檔案和個人資料,作業系統物件和已安裝程式以及網路活動安全,本程式使用不同的模組來保護每個物件,打開保護中心,您可以查看詳細的保護功能.
- 新的應用程式控制，可以快速訪問保護設定的管理，這些設定防止應用程式執行危險動作，監控訪問隱私資料。該項還允許在沙箱防護運行應用程式。
- 工具中心的精靈和工具，幫助執行特殊的安全任務。

電腦保護概念

Kaspersky Internet Security 使您的電腦得到安全保護，使它免受已知威脅，新的威脅，駭客和入侵攻擊，垃圾郵件和其它垃圾資訊的侵擾。每一類型的威脅都有單獨的應用程式模組來處理。這使設定更加靈活，為所有的模組設計簡單的設定選項來滿足特殊使用者或商業團體的需要。

Kaspersky Internet Security 包括：

- 保護模組，提供保護：
  - 檔和個人資料；
  - 系統；
  - 網路活動。
- 病毒掃描任務，掃描單獨的檔，資料夾，驅動器，區域範圍或整個電腦。
- 更新，確保使用最新的內部應用程式模組和資料庫來掃描惡意軟體，偵測駭客攻擊和垃圾資訊。
- 精靈和工具在 Kaspersky Internet Security 運行期間，精靈和工具使任務的執行更為須順利。

技術支援功能為程式和擴展資訊提供技術支援。

病毒掃描任務

除了持續打開自動保護免被惡意程式破壞外，特別重要的是用戶需要定期掃描電腦。這對排除安全性群組件沒被發現的惡意程式傳播的可能性是必要的，例如，因為安全級別設定過低。

Kaspersky Internet Security 有以下掃描任務：

- **物件掃描。** 掃描使用者選擇的物件。您可以掃描電腦系統中的任何物件。

- **完全掃描**。 徹底掃描整個系統。以下物件預設被掃描：系統記憶體，開機載入程式，系統備份，郵件資料庫，本機硬碟，移動存放裝置和網路磁碟。
- **快速掃描**。作業系統啟動物件的病毒掃描。

更新

若要阻止任何網路攻擊，Kaspersky Internet Security 應該時更新，才可刪除新的病毒或其它惡意程式。更新模組正是為了這個目的。它處理應用程式資料庫和模組的更新。

更新引擎從卡巴斯基實驗室伺服器上下載資料庫和程式模組更新到本地資料夾，然後賦予其它電腦訪問的許可權，從而減少了網路流量。

資料檔案和線上安全保護

Kaspersky Internet Security 保護您的電腦防止遭受惡意程式和未經授權的訪問，盡力確保您在本地網路和互聯網上的安全。

受保護的對象分為以下三種：

- 檔案，個人的電腦資料，不同的輸入參數（用戶名和密碼）。這些物件均由檔案防護和免疫防護保護。
- 安裝在您電腦上的應用程式及作業系統。這些物件由郵件防護，網頁防護，即時通訊防護和免疫防護保護。
- 線上安全：使用線上付款系統，郵件保護來預防垃圾郵件和病毒等。這些物件由郵件防護，網頁防護，反釣魚來保護。

控制應用程式和資料檔案的許可權

Kaspersky Internet Security 將阻止應用程式破壞系統安全檔案，將即時監控應用程式的運行情況，將使用以下模組來保護系統安全：

- 安全中心。系統中應用程式活動的日誌，並管理應用程式的活動，都基於他們所屬的組別。每一個分組都有固定的一套規則。這些規則限制應用程式去獲取不同的資源。
- 隱私資訊控制。應用程式控制管理應用程式對於隱私資料的操作許可權。它們包括檔案，資料夾和註冊表項目，其中的設定包含重要資料的最常用的應用，以及使用者的檔案（ My Documents 資料夾，cookies，使用者的活動資訊）。
- 在沙箱防護運行的應用程式。沙箱防護為應用程式運行提供了一個虛擬環境，這樣可以更好地保護作業系統和應用程式安全。

精靈和工具

確保電腦的安全不是一項簡單的任務，這需要瞭解作業系統特點和利用其弱點的方式。除此以外，大量且多樣的關於系統安全的資訊使分析和處理變得困難。

為了說明解決各項保證電腦安全的任務，Kaspersky Internet Security 中包含了以下這組精靈和工具：

- 瀏覽器設定服務，對 Microsoft Internet Explorer 瀏覽器的設定進行分析，首要的一點是該服務是從安全角度出發來分析。
- 系統恢復服務，用於消除系統中惡意物件的蹤跡。
- 個人隱私清理服務，查找並清除系統中使用者活動的蹤跡和作業系統設定，這些設定可以收集使用者活動資訊。
- 救援光碟，當使用反病毒程式或惡意程式清除工具無法清除電腦中的病毒時，使用該程式。
- 弱點掃描，執行電腦診斷，掃描作業系統中和電腦上安裝的應用程式中的弱點。
- 虛擬鍵盤，防止對鍵盤上輸入資料的攔截。
- 網路包分析，攔截網路資料封包並分析其中詳情。
- 網路監控，顯示了您電腦上網路活動的詳情。

程式支援功能

應用套裝程式含一組支援功能。設計這些功能是為了使電腦的保護處於最新狀態，擴展應用程式的性能，以及在使用過程中為您提供幫助。

資料檔案和報告

在應用程式運行期間，每個保護模組，掃描任務，或應用程式更新任務都會建立報告。它包括執行動作和運行結果的資訊；使用這些資訊，您可以詳細瞭解本程式是如何工作的。如果有問題，您可以發送報告給卡巴斯基實驗室，我們的工作人員可以根據情況解決問題。

Kaspersky Internet Security 將所有可疑的檔案移動到特別的存儲區-隔離區。它們被加密存儲在隔離區，以避免感染您的電腦。您可以掃描這些物件，恢復它們，刪除它們，

或者添加新的檔案到隔離區。病毒掃描結束後，所有被證明未感染的檔將自動恢復到原來的位置。

被清除或刪除的物件副本存儲在備份區。為了恢復檔案或圖片，需要為它們建立副本。這些備份副本也會被加密存儲，以避免感染。

您可以從備份區還原一個檔案到原來的位置，或刪除一個副本。

授權許可文件

只有啟動程式後，您才可以獲得完整保護功能和技術支援，授權許可檔詳細說明瞭授權的有效期以及可安裝的電腦數目。點擊左下角的授權，您可以查看該授權檔的詳細資訊，您也可以購買或續期授權檔。

技術支援

所有已註冊用戶可以享有我們的技術支援服務。為了獲悉技術支援，請使用技術支援功能。

點擊相應的連結您可以訪問卡巴斯基用戶的論壇，給技術支援發送一個錯誤報告，或者通過填寫一個指定的線上表格來給予回饋意見。

您也可以訪問線上技術支援服務，個人使用者服務專區；我們的工作人員將很樂意為您提供關於應用程式的電話技術支援。

安裝 Kaspersky Internet Security

使用安裝精靈以互動模式安裝 Kaspersky Internet Security。

在安裝之前，建議您關閉所有當前運行的應用程式。

若要安裝 Kaspersky Internet Security ，運行產品 CD 中的安裝檔案 (帶有.exe副檔名)。

從互聯網下載的安裝檔案安裝 Kaspersky Internet Security ，與從 CD 安裝應用程式是一樣的。

之後，將搜索 Kaspersky Internet Security 的安裝包(帶有.msi 副檔名的檔案)，如果發現安裝檔案，將在卡巴斯基實驗室的伺服器上檢查最新版本。如果沒有發現安裝包檔案，您需要下載它。下載完成後，Kaspersky Internet Security 開始安裝。如果取消下載，應用程式安裝將以標準模式進行。

安裝程式使用一系列標準的視窗執行，每個視窗包含一些按鈕控制安裝過程。以下為按鈕的簡單描述:

- **下一步 –** 接受動作，進行下一步安裝。
- **後退 –** 返回安裝的前一步驟。
- **取消 –** 取消安裝。
- **完成 –** 完成應用程式安裝。

下面我們詳細討論每一步安裝。

步驟 1. 檢查最新版本

安裝之前，應用程式在卡巴斯基實驗室的更新伺服器上搜索有無 Kaspersky Internet Security 的新版本。

如果沒有新版本，當前版本的安裝精靈開始運行。

如果發現新版本，您可以下載並安裝新版本。如果新版本的安裝被取消，當前版本的安裝精靈開始運行。如果您決定安裝新版本，安裝檔案下載到本地電腦後，安裝精靈將自動運行。

步驟 2. 驗證系統需求

安裝 Kaspersky Internet Security 之前，安裝精靈會檢查作業系統是否滿足安裝需求。此外，還會檢查所需的軟體和軟體安裝許可權。

如果有任一部份不滿足條件，螢幕上會顯示相應的通知。因此，安裝卡巴斯基實驗室的產品之前，建議您使用 Windows 的更新服務安裝所需的系統更新和所有需要的程式。

步驟 3. 選擇安裝類型

如果您的系統完成符合要求，而且沒有發現新版本或者您取消安裝新版本，安裝精靈將安裝當前版本。

該步驟，您需要選擇最適合您的安裝類型：

- 快速安裝。如果您選擇該項，整個程式根據卡巴斯基實驗室專家的建議安裝在您的電腦上，安裝完成之後，程式安裝精靈將會啟動。
- 自訂安裝。您可以選擇希望安裝的程式模組，指定程式要安裝的資料夾，使用特殊精靈啟動程式，並設定程式。

如果您選擇了第一項，應用程式安裝精靈可以讓您查看授權授權合約和 Kaspersky Security Network 資料收集聲明。之後，應用程式將被安裝在您的電腦上。

如果您選擇了第二項，需要輸入或確認安裝每一步的資訊。

繼續安裝，點擊下一步按鈕。取消安裝，點擊取消按鈕。

步驟 4. 查看授權文件合約

在這一步驟中，您可以查看您和卡巴斯基實驗室之間的授權文件。

請仔細的閱讀該協議，如果您接受該協議中的每一項，請點擊**我同意**按鈕。將繼續安裝該程式。

若要取消安裝，請點擊**取消**按鈕。

步驟 5. Kaspersky Security Network 資料收集聲明

在這一步驟中，您將可以加入到 Kaspersky Security Network 中。加入到這一個計畫包括發送您的電腦上偵測出的新威脅的相關資訊到卡巴斯基實驗室，發送包含 Kaspersky Internet Security 為您的電腦分配的 ID 號碼和系統資訊。而且，公司承諾不洩露任何隱私資料。

查看 Kaspersky Security Network 資料收集聲明。如果您接受加入這個專案，請選擇**我接受加入 Kaspersky Security Network 條款**方塊。

點擊**下一步**按鈕，將繼續進行安裝。

步驟 6. 選擇目的檔案夾

此安裝精靈的步驟僅適用於自訂安裝類型（詳見步驟 3.選擇安裝類型）。

在這一個安裝步驟中，您可以指定安裝 Kaspersky Internet Security 的安裝資料夾。以下是預設設定的路徑：

- **<drive> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009** – 針對32 bit 系統。
- **<drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2009** – 針對 64 bit 系統。

您可以另外指定其他的資料夾作為目標路徑，點擊瀏覽按鈕，並在資料夾選擇視窗中選擇資料夾，或者在相應的輸入區域中輸入對應的路徑。

如果您是手動的輸入安裝程式的資料夾完整路徑，請您記住這個路徑。該路徑中可能包括 200多個字元或者一些特殊字元號。

如繼續安裝，請點擊**下一步**按鈕。

步驟 7. 選擇所需要安裝的程式模組

此安裝精靈的步驟僅適用於自訂安裝類型（詳見步驟 3. 自訂安裝類型）。

若選擇自訂安裝，您需要指定需要的 Kaspersky Internet Security 的程式模組安裝到你電腦上。預設的情況下，所有的 Kaspersky Internet Security 的模組均會被選擇安裝，包括保護模組，掃描任務和更新任務。

若想要決定安裝哪個模組，請首先查看與這個模組相關的資訊。這樣的話，從清單中選擇組件並閱讀其下麵對應的資訊。資訊中包含簡單的說明，以及安裝這一模組所需的磁碟空間。

若要取消安裝一個模組，打開模組名字旁邊圖示所對應的上下文功能表，並選擇 **“** X **”** 。注意，一旦您取消安裝一些模組，您就有可能受到大量的危險程式的侵襲。

若要選擇安裝一個模組，打開模組名字旁邊圖示所對應的上下文功能表，並選擇將**在本機硬碟安裝該功能**項。

當您完成選擇所需要的安裝的模組後，點擊**下一步**按鈕。若要所安裝的預設組件清單， 點擊**重新開機**按鈕。

步驟 8. 關閉MICROSOFT WINDOWS 防火牆

該步驟僅適用於那些將 Kaspersky Internet Security 安裝在已啟用 Microsoft Windows 防火牆的電腦。

在安裝 Kaspersky Internet Security 的這一步驟中，因為 Kaspersky Internet Security 的防火牆可以針對您的網路活動進行全面的保護，並且沒有必要開啟附加的資源去佔用系統資源，所以您可以禁用 Microsoft Windows 的防火牆。

如果您希望使用防火牆作為網路活動的主要活動工具，點擊**下一步**按鈕。 Microsoft Windows 防火牆將自動關閉。

如果您想使用 Microsoft Windows 防火牆保護您的電腦，選擇啟用 **Microsoft Windows** 防火牆。在這樣的情況下，將安裝並啟動 Kaspersky Internet Security 的防火牆模組以避免程式操作過程中的衝突。

步驟 9. 使用之前的程式記錄進行安裝

在這一步驟中，您可以決定是否需要在將來的工作中使用舊的設定和程式的資料庫 **-** 前提是在移除上一個版本的 Kaspersky Internet Security 之後，在您的電腦上保存有原來的設定和資料庫。

讓我們詳細瞭解下如何使用上述功能。

您可以選擇程式運行設定，**iswift** 和 **ichecker** 資料，垃圾郵件防護資料庫

步驟 10. 查找其他反病毒程式

在這一步驟中，精靈會檢查其他的可能與 Kaspersky Internet Security 衝突的反病毒程式，包括其他的卡巴斯基實驗室的程式。

一旦在您的電腦中發現其他的反病毒程式，會將其列在電腦螢幕上。由您決定是否將其卸載及繼續安裝 Kaspersky Internet Security。

您可以在被偵測出來的反病毒程式下面選擇刪除的模式（自動或手動）。

一旦檢查出 Kaspersky Internet Security 2009 也包含在反病毒程式的清單中，建議您將它手動移除時，同時保存關鍵的檔案。您可以使用程式的記錄升級版本。也同樣建議您保存隔離區中的資料和備份的檔案；這些物件將被自動的歸還到升級版本的隔離區中。

如果在安裝 2010 版本時自動移除 2009 版本的程式，原版本中的啟動資訊會繼續沿用至即將安裝的 2010 版本中。

若繼續安裝，請點擊**下一步**按鈕。

步驟 11. 安裝的最後準備

該步驟是為完整安裝 Kaspersky Internet Security 作準備。

在自訂安裝（詳見**"**步驟 3.選擇安裝類型**"**）程式時，建議您不要勾選**保護安裝程式**這一欄。一旦在安裝程式的過程中出現任何錯誤，程式開啟的保護能夠允許您執行正確的安裝步驟的回滾。當您再次進行安裝時，推薦您不勾選這一欄。

若使用 *Windows* 遠端桌面 進行遠端安裝時，建議您不要勾選保護安裝程式這一欄。一旦勾選了這一欄，安裝程式就有可能出現安裝不完整或者執行錯誤等情況。

若繼續安裝，請點擊**安裝**按鈕。

當安裝 Kaspersky Internet Security 的模組時，它會攔截網路流量，當前的網路連接將被終止。一段時間之後將會自動恢復中止的連接。

步驟 12. 完成安裝

安裝完成後，視窗中會顯示完整安裝 Kaspersky Internet Security 相關資訊。

下一個步驟是程式的設定。設定精靈（詳見**"**程式設定精靈**"**）將有助於您快速正確的設定 Kaspersky Internet Security 。

點擊**下一步**按鈕轉至程式的設定視窗。

使用入門

卡巴斯基實驗室建立 Kaspersky Internet Security 的其中一項主要目的就是想為應用程式提供簡易設定。這就可以使不同的電腦知識的使用者在安裝程式之後不用浪費太多的時間便能保護他/她的電腦。

為了使用者的方便，我們竭盡全力整合程式設定精靈（詳見"程式設定精靈"）的介面。遵循該精靈的操作指南，您可以啟動 Kaspersky Internet Security ，修改更新設定，設定密碼限制程式的變更。

在安裝 Kaspersky Internet Security 之前您的電腦可能會感染到一些惡意程式。若要刪除這些惡意程式，請運行完整掃描。

由於惡意軟體的操作和系統故障等因素，您的電腦的設定有可能被損壞。運行弱點掃描任務（詳見"弱點掃描"）檢查已安裝軟體的弱點以及不正確的系統設定。

在程式剛剛安裝完成時，反病毒庫可能已經過期。更新程式能有效發現新病毒。

垃圾郵件防護模組包括了 Kaspersky Internet Security 所使用的自我學習模式來偵測垃圾郵件。您可以利用學習精靈設定垃圾郵件防護模組。

在完成如上操作之後，Kaspersky Internet Security 就會準備開始運作。

程式設定精靈

在安裝完成之後開始運行程式設定精靈。基於您的電腦的特徵以及基礎上進一步的設定。

程式設定精靈的介面是一系列 Windows 的步驟，您可以使用**上一步**按鈕和**下一步**按鈕，或在關閉的時候使用**取消**按鈕。

步驟 1. 啟動程式

啟動程式的過程中。程式將根據該授權許可時間，來計算出授權使用的時間範圍。

Key 檔案會在啟動的過程中下載。Key 檔案已包括了允許 Kaspersky Internet Security 運行的必要授權資訊：

- 技術支援資訊；
- Key 檔的名字和序號，以及產品的有效期。

您需要網際網路去啟動應用程式。

若要在啟動的過程中獲得 key 檔，首先您需要有一個啟動碼。啟動碼是作為您購買該程式的憑證。Kaspersky Internet Security 將提供給您如下的啟動方式：

- 啟動商用授權。如果您已經購買了商用的授權許可檔，您可以選擇這種啟動方式，而且前提是您需要有一個啟動碼。用這個啟動碼，您可以獲得一個對 Key 檔案。
- 啟動試用授權。如果在決定購買一個商用的授權許可檔之前，您可以使用啟動試用授權這種方式。您將獲得一個 30日免費的 key 授權檔。
- 稍後啟動。 如果您選擇該操作，Kaspersky Internet Security 將會跳過啟動這一步驟。接下來程式將安裝在您的電腦上，所有的模組均可用，除了更新（在安裝完成之後，您僅可以更新一次）稍後啟動這一操作僅在程式完成安裝後第一次打開啟動精靈時可見。

如果已經安裝過 Kaspersky Internet Security ，之後又卸載了，而且保存了啟動資訊，則會跳過該啟動步驟。在這種情況下，設定精靈將會自動張已記錄的授權相關資訊，顯示在精靈的視窗中。

啟動商用版本

如果您選擇該操作，由於要通過卡巴斯基實驗室進行啟動，所以需要有網際網路的連接。

啟動是需要輸入啟動碼的。如果您購買的是盒裝產品（零售版），那麼啟動碼將會在包裝內找到。

啟動碼是一串被分隔成四個小組，每小組由五個字元構成。例如，XXXXX-XXXXX-XXXXX-XXXXX。注意，請使用拉丁文輸入這段字元。

啟動精靈通過互聯網連接到卡巴斯基實驗室的啟動伺服器上，並向其發送您所提供的啟動碼，然後驗證啟動碼。如果啟動碼成功的通過驗證，該精靈就會收到一個 key 檔並將其自動安裝。視窗中會顯示詳細的授權資訊。

一旦啟動碼沒有通過驗證，您會在螢幕中看到相應的資訊。這種情況下，您可以與您購買軟體的經銷商取得聯繫並獲得相應的資訊。

一旦超過了啟動碼啟動次數的最大限度，相應的資訊也會在螢幕上顯示出來。啟動過程就將被阻斷，程式會向您提供連接到卡巴斯基實驗室技術支援服務網頁的連結。

如果在連接啟動伺服器的過程中出現任何錯誤，從而導致您不能順利的獲得key檔，請您聯繫技術支援。

啟動試用版本

如果在決定購買一個商用的授權許可為檔之前，您可以使用啟動試用版本進行啟動。您將獲得一個30日免費的 key 授權檔。當試用期限已滿，就將不可以再啟動試用版第二次。

如果在連接啟動伺服器的過程中出現任何錯誤，從而導致您不能順利的獲得key檔，請您聯繫技術支援。

完成啟動

在成功啟動 Kaspersky Internet Security 之後，啟動精靈將會向您發出通知。此外，還會提供授權許可的相關資訊：授權許可的類型（商用，試用，等），產品的有效期，以及能夠同時使用該授權許可檔的電腦數量。

步驟 2. 選擇保護模式

選擇 Kaspersky Internet Security 所提供的保護模式。

以下為兩種可用的保護模式選擇：

- *自動模式。* 一旦發生了什麼重大的事件，Kaspersky Internet Security 會根據卡巴斯基實驗室的推薦自動執行操作。一旦發現威脅，程式將試圖為被感染物件清除病毒；如果清除病毒失敗，程式將刪除被感染物件。受懷疑的物件將被跳過而不會被執行操作。快顯視窗資訊向使用者通知新事件。
- 互動模式。 在這一模式中，程式會按照您指定的方式對事件做出反應。一旦某一事件需要引起您的關注，程式會彈出通知並提出解決方案供您選擇操作。

無論您選擇哪種保護模式，偵測到感染事件都會顯示出相應的通知。

步驟 3. 設定程式更新

如果您選擇了快速安裝模式，程式設定精靈這一步驟將被跳過。在這一步驟中程式設定編輯將為預設值。

對您的電腦的保護的品質取決於資料庫和程式模組的更新。在該視窗中，設定精靈會要求您設定 Kaspersky Internet Security 的更新模式以及編輯計畫設定。

- 自動更新。 Kaspersky Internet Security 會在指定的時間內從更新伺服器核對更新包。一發現新的更新數據庫，程式會自動下載並安裝到電腦上。這是預設的模式。
- 按排程更新（時間間隔可能會根據排程的設定而改變）根據建立的排程自動運行更新。點擊設定按鈕，您可以在打開的視窗中更改排程設定。
- 手動更新。 如果您選擇該操作，您將根據您的需要手來設運行程式更新。

注意，新安裝 Kaspersky Internet Security 的時候，資料庫和程式模組可能均已過期。所以，程式會建議您立即取得 Kaspersky Internet Security 最新的更新。若要獲取最新版本，請您點擊立即更新按鈕。屆時，程式會在更新伺服器上下載所需的更新，並安裝到您的電腦上。

如果安裝程式中的資料庫已經過期了，更新包可能會很大，那麼就有可能導致效多的網路流量。

若您想切換到編輯更新設定（例如，選擇更新源，使用使用者的帳戶運行更新程式，以及將更新服務指向本地更新源），點擊設定按鈕。

步驟 4. 限制應用程式的存取權限

如果您選擇了快速安裝模式，程式設定精靈這一步驟將被跳過。 在這一步驟中程式設定編輯將為預設值。

由於一台個人的電腦上可能由幾個人共用，並且一些模組可以暫停保護，所以您需要選擇密碼保護來控制 Kaspersky Internet Security 的使用權限。使用密碼，可以防止未經授權的人對 Kaspersky Internet Security 一些模組停用或修改設定等操作。

若要使用密碼保護，則勾選啟用密碼保護這一欄並在密碼和確認新密碼欄中輸入您要設定的密碼。

以下，您可以指定使用密碼保護的範圍：

- 更改應用程式設定 - 當使用者希望儲存對 Kaspersky Internet Security 的設定更改時，需要輸入密碼。
- 退出應用程式 - 當使用者希望退出程式時，需要輸入密碼。

步驟 5. 選擇所偵測的威脅類型

如果您選擇了快速安裝模式，程式設定精靈這一步驟將被跳過。 在這一步驟中程式設定編輯將為預設值。

在這一步驟中，您能夠選擇 Kaspersky Internet Security 檢查威脅的類型。Kaspersky Internet Security 監察能夠對您的電腦造成危害的程式，包括病毒，蠕蟲和木馬。

步驟 6. 禁用DNS

如果您選擇了快速安裝模式，程式設定精靈這一步驟將被跳過。在這一步驟中程式設定編輯將為預設值。

DNS緩存可以大大的減少您的電腦接入互聯網所用的時間。然而，與此同時，這也是一個危險的漏洞，利用這一項，駭客們很容易獲取您的資料資訊。

勾選禁用**DNS**緩存欄以提升您電腦的安全級別。

步驟 7. 系統分析

在這一階段，會搜集 Microsoft Windows 程式的相關資訊。這些程式被添加到信任程式清單中，它們在系統中執行操作的時候不受任何限制。

步驟 8. 關閉安裝精靈

精靈的最後一個視窗將通知您完成程式的安裝。若要立即運行 Kaspersky Internet Security ，請確保**啟動 Kaspersky Internet Security** 被勾選，並點擊**完成**按鈕。

選擇網路類型

在 Kaspersky Internet Security 安裝完成之後，防火牆模組將分析您電腦的網路連接活動。每個網路連接都將被分配到一個允許其網路活動範圍的狀態。

如果對於 Kaspersky Internet Security 的操作，您選擇的是互動模式（詳見步驟 2"選擇防護模式
），在每一次新的網路連接之後，都會向您發出通知。您可以在通知視窗中為新的網路連接選擇狀態：

- 公共網路。這種狀態下的網路連接是禁止別人從外網訪問您的電腦。訪問公共的資料夾以及共用印表機也是禁止的。推薦在連接到 Internet 的網路中時使用該網路狀態。
- 本機網路。這種狀態下的網路連接是允許訪問公共的資料夾以及共用印表機的。建議您指定被保護網路的狀態，例如，公司網路。
- 信任網路。這種狀態下的網路連接是不受限制的。建議您只對絕對安全區域指定該狀態。

對於每一種網路狀態，Kaspersky Internet Security 使用與之相關的規則組去管理網路活動。必要的話，在隨後的操作中您可以更改最初的網路連接狀態的設定。

更新程式

您需要一個用於更新 Kaspersky Internet Security 的網路連接。

Kaspersky Internet Security 所依賴的資料庫中包含一些威脅的數位簽章，典型的垃圾郵件片語，以及網路攻擊的相關描述。在 Kaspersky Internet Security 完成安裝的時候這些資料就可能已經過期了，因此卡巴斯基實驗室要對資料庫和程式模組都會自動定期的更新。

在程式設定精靈中，您可以選擇更新的啟動模式（詳見步驟 3"設定程式更新"）預設的情況下，Kaspersky Internet Security 會自動到卡巴斯基實驗室的更新伺服器上自動搜索更新來源。若伺服器上有新的更新資來源，程式會以背景模式完成下載並安裝。

如果安裝程式中的資料庫已經過期了，更新包可能會很大，那麼就有可能導致效多的網路流量。

若要確保您的電腦的病毒資料庫不是過期，建議您在完成安裝 Kaspersky Internet Security 之後立即運行更新。 若要手動更新 Kaspersky Internet Security ，則： 1. 打開程式的主視窗。 2. 在視窗的左側選擇**我的更新中心**部分。 3. 點擊**開始更新**。

掃描病毒

惡意軟體的開發者會竭盡全力來掩飾他們的程式，所以您就可能注意不到您電腦中的惡意軟體。

一旦安裝了 Kaspersky Internet Security ，它會對您的電腦自動的執行快速掃描。該任務會在作業系統啟動過程中，查殺被載入物件中的惡意程式。

卡巴斯基實驗室的專家還建議您執行全硬碟掃描任務。

I 若要開啟病毒掃描任務，請執行如下操作：

1. 打開程式的主視窗。
2. 在視窗的左側選擇**掃描我的電腦**部分。
3. 點擊**開始完整掃描**按鈕開始掃描。

掃描電腦弱點

系統故障或者惡意程式活動造成的有害行為導致作業系統被破壞。另外，您電腦上安裝的程式的弱點可能被入侵者利用並破壞您的電腦。

為了偵測並清除這些安全問題，卡巴斯基實驗室專家建議您在安裝完程式後啟用弱點掃描。弱點掃描查找本地安裝程式的弱點以及作業系統和瀏覽器設定的異常和損害。

- 啟動弱點掃描：

  1. 打開程式主視窗。
  2. 在視窗的左側選擇**掃描我的電腦**部分。
  3. 點擊打開弱點掃描視窗按鈕。
  4. 打開的視窗，點擊開始弱點掃描按鈕。

管理授權許可文件

Kaspersky Internet Security 需要一個有效的授權許可來啟動。當您購買程式時會提供一個授權啟動碼。有了授權啟動碼，您從購買並安裝好它的那天起才具有程式的使用權。授權啟動碼包含資訊: 授權類型， 到期日期，可安裝的電腦數量。

如果沒有授權啟動碼，除非啟動了試用序號，那麼程式將運行在只能進行一次更新，之後不能下載任何新的更新檔。

如果啟動了程式的試用序號，當試用期限過期時，將不能運行該程式。

當授權啟動碼過期時，該程式可以繼續運行，只是您不能繼續更新資料庫。和以前一樣，您還是可以進行病毒掃描並使用保護模組，但是只能使用過期的資料庫。當您的授權許可檔過期後，我們不能確保您的電腦免受新病毒的侵害。

為了保護您的電腦不被新病毒所感染，我們建議您更新授權許可檔。應用程式會提前兩周通知您授權許可檔即將到期。在此期間啟動應用程式時，螢幕上也會顯示一條消息來提醒您。

當前使用的授權許可資訊被顯示在授權管理視窗內：授權類型(商用、商用訂購、試用、測試)，電腦數量，到期日期，和剩餘天數。

查看應用程式授權授權合約的方法是，點擊查看最終用戶授權授權合約鍵。若要刪除許可檔，點擊 **”X”** 按鈕。若要啟動新的許可檔，點擊啟動新授權按鈕。

使用**購買授權**(更新授權)按鈕，您可以在卡巴斯基實驗室網站上進行購買。

加入 Kaspersky Security Network

每日出現大量的新型威脅。為了方便搜集新威脅，卡巴斯基實驗室邀請您使用 Kaspersky Security Network 服務。

使用 Kaspersky Security Network 需要發送下面的資料到卡巴斯基實驗室：

- Kaspersky Security Network 分配給您的電腦特有的識別字，用來描述您電腦的硬體設定，並不包含其它資訊。
- 被 Kaspersky 程式偵測到威脅的資訊。 資訊結構和偵測到的威脅類型。
- 系統資訊：作業系統的版本，安裝的服務包，服務和驅動資訊，郵件用戶端，瀏覽器擴展部分，安裝的卡巴斯基實驗室程式版本。

Kaspersky Security Network 也包含下麵資訊的擴展資料：

- 您電腦上的執行檔和程式簽署；
- 您電腦上運行的程式。

統計資訊在更新完成後發送。

卡巴斯基實驗室保證不搜集和發佈使用者的個人資料來執行 Kaspersky Security Network。

- 若要設定統計發送設定：

  1. 打開程式設定視窗。
  2. 在視窗左邊選擇客戶意見。
  3. 選 **“✓”** 中我同意加入 Kaspersky Security Network 核取方塊來確認您加入 Kaspersky Security Network。

安全管理

電腦保護中出現問題，將會通過電腦保護狀態來顯示。保護狀態圖示及其面板的顏色變化，將指示出當時的保護狀態。一旦保護系統中出現問題，我們建議您立即修復。



圖*1:* 電腦保護的當前狀態

您可以在狀態面板查看問題發生的狀態，可在這裡查看描述和可能解決的方法。(詳見下圖)；您可以點擊狀態圖示或保護狀態面板上顯示(詳見上圖)。



圖*2:* 解決安全問題

標籤顯示當前問題清單，問題包括它們的危險程度，首先，嚴重的威脅(例如，紅色的狀態圖示)，不嚴重的威脅 – 黃色的狀態圖示； 最後是一些提示資訊。 每個問題都有詳細的描述，同時還可以對其採取以下的操作：

- 立即修復。使用相應的按鈕，您可以立即對問題進行修復，這也是建議的操作。
- 隱藏訊息。如果有某些原因，不可能立即修復該問題，那麼您可以點擊隱藏訊息按鈕，稍後解決。

請注意，對於嚴重問題，不提供該選項。這一類問題包括，無法清除惡意物件，一個或多個模組出錯，或是程式出錯。

如要再次顯示隱藏的資訊，選 “✓” **顯示隱藏訊息**方塊。

保護狀態

執行 Kaspersky Internet Security 模組或執行病毒掃描任務都將記錄在電腦保護狀態摘要資訊中。您可以知道多少危險和可疑物件被程式偵測到，並是否已進行清除或隔離。 電腦保護狀態警告使用者關於惡意物件偵測，並更改保護狀態顏色。如果惡意物件被偵測到，圖示顏色和麵板上的顏色將變成紅色。這種情況下，所有出現的威脅將立刻處理。

Ø 若要查看電腦保護狀態：

1. 打開程式主介面。
2. 點擊<u>報告</u>連接。

Ø 在電腦保護中清除發生的問題*:*

1. 打開程式主視窗。
2. 點擊<u>報告</u>連結。
3. 在打開視窗的**狀態**中執行需要的操作。如要再次顯示隱藏的資訊，選 “✓” **顯示隱藏訊息**方塊。

I 對偵測到的物件執行操作。

1. 打開程式主視窗。
2. 點擊報告的連結。
3. 在打開視窗的已偵測到的威脅標籤中，在清單中選擇需要的物件或右擊它。
4. 在打開的目錄功能表中選擇需要的操作。

暫停防護

暫停防護意味著在一個特定的時期內臨時禁用所有防護模組。

暫停防護，所有的防護模組都將被暫停。下麵將顯示程式暫停後的狀態：

- 在工作列程式圖示變為灰色；
- 程式主視窗的圖示顯示為紅色。

如果電腦正與網路連接，當保護被暫停時，將會顯示一條關於終止當前連接的通知。

➢ 若要暫停電腦保護：

1. 在應用程式的快顯功能表中選擇暫停保護。
2. 在打開的暫停防護視窗， 選擇暫停的時間，經過這段時間後，防護會自動啟用：

- 下一次暫停 **<暫停防護時間> –** 防護將會在這段時候後被啟用。使用下拉式功能表來選擇時間值。
- 重新開機後恢復防護 **–** 保護將在系統重啟後啟用。
- 手動恢復防護 – 保護只有由您手動來啟動。想要啟用保護，在應用程式快顯功能表選擇回復防護。

保護模組

檔案防護

檔案防護防止電腦檔案系統被感染。在您啟動作業系統時載入檔案防護並開始在記憶體中運行，該功能掃描所有打開的，保存的和執行的檔案。

預設時，檔案防護僅掃描新建和更改過的文件。安全級別決定了掃描檔案的方法。如果檔案防護偵測到威脅，它將執行指定的操作。

您電腦的檔案和記憶體保護等級由以下固定設定決定：

- 新增保護範圍；
- 掃描方式；
- 掃描複合檔案 (包括掃描大的複合檔案)；
- 掃描摸式；
- 允許根據排程暫停模組或選擇程式操作。

卡巴斯基實驗室專家建議您不要自己自訂製檔案防護設定。大部分情況下，更改安全級別就已經足夠了。若要恢復檔案防護的預設設定，選擇一個安全級別就可以了。

若要修改檔案防護設定：

1. 打開程式介面，點擊視窗頂部的<u>設定</u>連結。
2. 在打開的視窗的**保護**部分選擇**檔案防護**模組。
3. 為您選擇的模組點擊**設定**按鈕。
4. 在相應的設定中做必要的更改。

模組運行規則

當您打開電腦，電腦將在記憶體中運行檔案防護，它將掃描所有被打開，被保存和被運行的檔案。

預設的情況下，檔案防護只掃描最新的或是已修改的檔；換句話說，就是在最近的一次掃描結束後，只掃描新添加的和已經修改的檔案。檔案將通過以下的方式掃描：

1. 模組攔截使用者或任意程式試圖訪問檔案的行為。
2. 檔案防護掃描 iChecker 和 iSwift 資料庫中被攔截檔的資訊，然後基於被檢查的資訊來決定是否掃描該檔案。

掃描包含以下步驟:

1. 掃描檔案中的病毒 ，Kaspersky 通過對比應用程式資料庫來偵測惡意程式。該資料庫中包含所有的惡意程式和目前已知威脅的描述和處理它們的方法。
2. 經分析，程式可能採取如下的操作：

A. 如果在檔案中偵測到惡意程式碼，檔檔案防護將阻止這個檔案，建立備份，同時試圖去清除病毒。如果惡意程式被成功地清除，該檔案可以重新被使用，而如果清除惡意程式的操作失敗，這個受感染的檔案將被刪除。

B. 如果在檔案中偵測到一段疑似惡意程式的代碼時，該檔案有可能被清除病毒，並將其發送到隔離區。

C. 如果在檔案中沒有發現惡意程式碼，那麼該檔案將直接被恢復。

一旦偵測到已感染物件或潛在己被感染的檔案，程式將通知您選擇如何操作：

- 隔離新威脅，稍後使用更新的資料庫來處理；
- 刪除物件；
- 略過（如果您確定該檔案不包含惡意程式）。

郵件防護

郵件防護掃描用來偵測寄出及寄入的郵件是否存在惡意物件。它在作業系統啟動期間載入到電腦記憶體並且一起運行，掃描所有通過POP3，SMTP，IMAP，MAPI和NNTP協定接收的郵件。

通過已經設定的安全級別來對郵件進行掃描。如果郵件防護偵測到一個威脅，它將執行指定的操作。郵件掃描時使用的規則通過一組設定來定義。該設定可以分為下列四類：

防護範圍；
使用啟發式分析；
掃描複合檔案；

附件過濾。

卡巴斯基實驗室專家不推薦您親自設定郵件防護的設定。大多數情況下，根據需要選擇不同的安全級別已經足夠保證安全。想要恢復預設的郵件防護設定，選擇安全級別的其中一個。

若要修改郵件防護設定：

1. 打開主程序視窗，點擊視窗上部的**設定**連結。
2. 在打開的視窗**保護**部分選擇**郵件防護**模組。
3. 為您選擇的模組點擊設定按鈕。
4. 在組件設定中做必要的更改。

模組運行規則

程式有一個專門的模組用來防禦寄出及寄入的郵件中的危險物件：郵件防護。郵件防護在作業系統啟動時載入並一直運行，掃描所有通過POP3，SMTP，IMAP，MAPI和NNTP協議接收的郵件，以及掃描POP3和IMAP安全連接(SSL)。

在工作列通知區域的程式圖示就是模組操作的指示器，當掃描郵件時，圖示顯示為。

預設情況下，郵件保護是這樣運作的：

1. 每封用戶收到的或發出的郵件被該模組掃描。
2. 郵件被分成三部分：郵件標題，正文和附件。
3. 掃描正文和附件（包括OLE物件）中的危險物件，利用程式中的資料庫進行啟發式掃描偵測惡意物件，資料庫包含所有已知惡意程式的描述和處理它們的方法。啟發式掃描可以偵測到沒有加入資料庫中的新病毒。
4. 病毒掃描完成後，進行以下操作：

    如果郵件正文或附件包含惡意程式碼，郵件防護會阻止該郵件，建立它的備份並嘗試清除病毒。如果病毒被成功清除，它將重新變為可用的。如果病毒清除失敗，感染的物件會被刪除。在郵件防護掃描之後，郵件主題行會插入一個特定的文字，表明該郵件被處理過。

    如果在正文或附件裡偵測到的代碼看起來是惡意的但是不能確定，郵件的可疑部分會被送到隔離區。

    如果郵件裡沒有發現惡意程式碼，將立即發送給用戶。

一個專門提供給 Microsoft Office Outlook 的外掛程式可以調整郵件規則。

如果您使用 The Bat ！，該程式可以與其它反病毒程式一起使用。在 TheBat ！裡直接設定郵件流量處理規則，並且取代程式的保護設定。

當與別的郵件程式（包括Microsoft Outlook Express，Windows Mail，Mozilla Thunderbird，Eudora，Incredimail）一起使用時。郵件防護根據SMTP，POP3，IMAP和NNTP協定傳遞的掃描郵件。

注意，在 Thunderbird 中，如果您使用篩檢程式將那些通過IMAP傳遞的郵件移出信箱，這些郵件將不被掃描。

網頁防護

當您使用網路時，電腦上的存儲資訊就會存在被危險程式感染的風險，當您下載免費軟體或瀏覽您認為安全的網站（在您訪問之前已經受到駭客攻擊）時，這些惡意程式就能滲入您的電腦。此外，只要您的電腦與網路連接，在您打開網頁和下載檔案之前，網路蠕蟲也可能侵入您的電腦。

網頁防護模組確保您安全地使用網路。它能保護由HTTP協定傳入您電腦的資訊，阻止危險腳本在您的電腦中執行。

網頁防護僅監控那些通過監控埠列表上的埠傳輸的HTTP流量。這些經常用來傳遞郵件和HTTP流量的埠列表包含在套裝程式裡。如果您使用的埠不在這個列表中，可以把它們添加到列表以保護通過它們的流量。

如果您在未保護區工作，建議您在連接互聯網時使用網頁防護來保護您的電腦。如果您的電腦運行在一個有HTTP流量過濾的防火牆保護的網路裡。網頁防護會為您使用互聯網提供充分的保護。

網頁防護僅使用安全級別的設定。如果網頁防護偵測到威脅，就會按照預定的操作執行。

您的網頁防護級別由下幾組設定值決定：

掃描方式設定：

決定網頁防護效率的設定（使用啟發式分析，掃描最優化）。 卡巴斯基實驗室專家建議您不要自己設定網頁防護設定。多數情況下，需要選擇不同的安全級別。

若要修改網頁防護設定*:*

1. 打開主程序視窗，點擊視窗上部的<u>**設定**</u>連結。
2. 在打開的視窗**我的防護**部分選擇網頁防護模組。

3. 為您選擇的模組點擊設定按鈕。

4. 在組件設定中做必要的修改。

模組運行規則

網頁防護保護通過HTTP進入電腦的資訊，並預防在電腦上執行危險腳本。

讓我們來詳細瞭解組件操作的設計。使用下面這個演算法來保護HTTP通信資訊：

1. 每個通過 HTTP 特定程式訪問的網頁或檔案都會被網頁防護攔截，並對其進行惡意程式碼分析。使用包含在 Kaspersky Internet Security 中的資料庫和啟發式掃描來偵測惡意物件。資料庫包含了對所有目前已知的惡意程式和處理它們的方法的描述。啟發式掃描可以偵測出資料庫中沒有的新病毒。
2. 通過分析，會出現下列處理方式：

   如果使用者訪問的網頁或物件包含惡意程式碼，它會停止訪問為該物件。並且會顯示一個通知，告知您此物件或網頁已經被感染。

   如果檔案或網頁不包含惡意程式碼，那麼用戶可以立即訪問它。

指令檔案根據下麵演算法進行掃描：

1. 每個運行網頁的腳本將被網頁防護截斷並分析其惡意程式碼。
2. 如果腳本中包含惡意程式碼，網頁防護將阻止它並彈出一個消息通知使用者。
3. 如果在腳本中沒有發現惡意程式碼，它將繼續運行。 腳本防護僅用於 Microsoft Internet Explorer 打開的網頁。

即時通訊防護

當前流行的即時通訊軟件已經給電腦安全帶來了潛在威脅。那些含有可疑網站 URLs 的資訊和那些被入侵者利用進行釣魚攻擊的資訊可能利用IM用戶端傳輸。惡意程式使用IM用戶端發送垃圾郵件資訊和URLs，盜取使用者的ID號和密碼。

即時通訊防護模組用來確保IM用戶端的安全性，它保護通過IM協定進入您電腦的資訊。

本程式確保各種即時通訊程式安全運行，包括 ICQ，MSN，AIM，Yahoo!，Messenge，Jabber，Google Talk，等等。

應用程式使用SSL協定。為了即時通訊防護掃描這些應用程式的流量，必需使用掃描加密連接。
在網路選項中選中 **"✓"** 掃描加密的連接。

本程式掃描即時通訊的流量。如果偵測到威脅，即時通訊防護會使用警告資訊替換含有威脅的資訊。

您的即時通訊流量保護等級決定分為以下幾組：

- 建立防護範圍的設定；
- 決定掃描方式的設定；

若要修改即時通訊防護設定：

1. 打開主程序視窗，點擊視窗上部的<u>**設定**</u>的連結。
2. 在打開視窗的**保護**部分，選擇**即時通訊防護**模組。
3. 在選擇組件的設定中作必要的更改。

模組運行規則

卡巴斯基反病毒包含一個模組，掃描通過即時通訊工具傳輸的資訊，叫即時通訊防護。它在作業系統啟動時載入，運行在電腦記憶體中。掃描所有入和出的資訊。

預設情況下，使用如下方法來進行即時通訊流量保護：

1. 每個接收和發送的資訊都被該模組攔截。
2. 即時通訊防護掃描資訊中是否含有危險物件或可疑網站或者釣魚網站的位址。如果偵測到威脅，資訊文本將被警告資訊替換。
3. 如果在資訊中沒有偵測到安全威脅，資訊對使用者是可用的。

通過即時通訊用戶端傳輸的檔在保存時會被檔案防護模組掃描。

應用程式控制

根據系統安全性因素，所有的程式可以分成三種：

安全。該組別包含由知名廠商開發並帶有數位簽章的應用程式。您可以允許該類程式做任何操作。

危險。該組別包含目前已知的威脅，必須阻止這些程式的活動。

未知。該組別包含一些由不知名開發者的並沒有數位簽章的程式。這些應用程式可能會或不會損害系統。使用並分析過它們的活動以後，您可以確定它們是否安全。在您確定一個未知程式是否安全之前，有必要限制它對系統資源的訪問。

安全中心報告會記錄程式執行的動作並按組監控應用程式的活動，每組都有規則可循，這些規則監控程式訪問各種資源，例如：

文件和資料夾；

註冊表；

網路位址；

執行環境。

當一個應用程式試圖訪問某資源時，該模組會確認該應用程式是否有存取權限，並使該程式按照指定的規則執行操作。

若要修改安全中心的設定，請執行如下步驟：

1. 打開主程序視窗並點擊視窗頂部的<u>**設定**</u>的連結。
2. 在打開的視窗的**防護**部分中選擇**應用程式控制**模組。
3. 在設定中對於您所選擇的模組根據需要進行更改。

您也可以執行如下操作：

1. 打開主程序視窗並選擇程式控制部分。
2. 在視窗右邊點擊<u>**應用程式活動**</u>的連結。
3. 在打開的**應用程式活動**控制視窗做必要的更改。

模組操作演算法

在第一次啟動程式時，將使用下面的規則分析程式：

1. 掃描病毒。
2. 驗證程式的數位簽章。如果數位簽章被確認，程式將添加到信任組。如果程式沒有數位簽章(或如果數位簽章被破壞，或添加到黑名單)，模組將進行下一步。
3. 當程式啟動時檢查 Kaspersky Internet Security 2010 資料庫中是否存在程式相關開機記錄，如果存在，則分配到相關組中，如果不存在則執行以下步驟
4. 發送程式執行檔的資訊到卡巴斯基實驗室伺服器已知程式資料庫。如果資料庫中已經包含記錄的資訊，程式將被添加到信任組。如果資料庫無法獲得(例如，沒有網路連接)模組將進行下一步。
5. 使用啟發式分析計算程式的威脅等級。等級如果較低將被添加到低限制組。如果程式等級高，Kaspersky Internet Security 將通知您，並將提示您選擇組別進行添加。

當這些掃描完成時，通知顯示最終的程式判斷。預設顯示程式被添加到信任組別的通知。
當程式重新啟動，程式控制會檢測完整性。如果程式沒有被更改，模組會應用現有的規則。如果程式被更改，程式控制會使用上面的規則描述分析。

沙箱防護運行的應用程式

沙箱防護在 Microsoft Windows XP x64 的電腦上不可用。

若要確保作業系統物件和使用者隱私資料的最大安全性，卡巴斯基實驗室使用在受保護的虛擬環境中運行協力廠商應用程式功能，也就是在沙箱防護運行。

當在沙箱防護運行時，建議您避免運行佔用記憶體比較大的程式

當在沙箱防護運行時，Microsoft Windows Vista x64 的電腦上特定應用程式的功能會被限制。如果這些程式被啟動了，相應的通知資訊會顯示在螢幕上。

在沙箱防護運行 IE 瀏覽器，確保瀏覽網路資源的安全性，包括防禦惡意入侵電腦和保護使用者隱私資料被未經授權的修改和刪除破壞，以及刪除網路會話過程中累積的物件：暫存檔案，cookies，歷史記錄，等。默認時，Microsoft Internet Explorer 包含在運行在沙箱防護的應用程式清單中。

對那些在沙箱防護保存過的或修改過的檔案，若您希望在標準模式下也可使用，您需要使用沙箱防護資料夾，當清除沙箱防護資料時，存儲在共用資料夾中的檔案不會被刪除。

建議您使用 Microsoft Windows 標準模式安裝您希望在沙箱防護運行的應用程式。

防火牆

Kaspersky Internet Security 包括一個專用的模組 - 防火牆，來保證內聯網和互聯網的安全。防火牆使用兩種類型的規則過濾所有網路活動：應用程式規則和封包規則。

防火牆分析您用來連接的電腦網路設定。如果應用程式工作在互動模式下，第一次連接時，防火牆需要您指定被連接網路的狀態。如果關閉了互動模式，防火牆根據網路類型，位址範圍和其它細則決定網路狀態。根據網路狀態，防火牆使用各種規則過濾網路活動。

若要修改防火牆設定：

1. 打開主程序視窗並點擊視窗上部**設定**的連結。
2. 在打開的視窗**防護**部分選擇防火牆模組。
3. 為您已經選擇的模組點擊**設定**按鈕。
4. 在打開視窗的**過濾規則**和**網路**標籤部分修改**防火牆**運行設定。

免疫防護

Kaspersky Internet Security 不僅可以防禦已知威脅，還可以防禦資料庫中還沒有的最新出現的威脅，該功能就是免疫防護。

免疫防護提供的預防技術可以避免浪費時間並且在新威脅危害您的電腦之前就將其控制。與基於資料庫記錄的分析代碼的反應技術相比，預防技術通過一系列特定程式執行的操作來識別新威脅。如果活動分析發現這些操作可疑，Kaspersky Internet Security 將阻止這個程式的活動。

所有應用程式都會進行活動分析，包括那些應用程式控制模組的**信任**組中的程式。為這些程式您可以禁用免疫防護的通知。

與應用程式控制模組完全不同的是，免疫防護對應用程式活動會立刻做出反應。

若要編輯免疫防護設定，請執行如下操作：

1. 打開主程序視窗並點擊視窗頂部<u>設定</u>的連結。
2. 在打開視窗的**保護**部分選擇**免疫防護**模組。
3. 在設定中為您選擇的組件做必要的修改。

網路攻擊防護

在作業系統啟動時將載入網路攻擊防護，並掃描接收的網路流量。一旦檢測到攻擊，本程式將阻止任何攻擊您電腦的網路活動。默認時，阻止持續一個小時。在攻擊發起時，螢幕上會顯示一則關於攻擊資訊的警告。

程式資料庫中提供對已知的網路攻擊描述和應對辦法。網路攻擊清單跟應用程式資料庫一起更新。

垃圾郵件防護

Kaspersky Internet Security 包括套裝程式含垃圾郵件防護模組，該模組能根據郵件用戶端的規則來檢測和處理垃圾郵件，當您收發郵件時節省您的時間。

垃圾郵件防護使用自我學習演算法，允許模組隨著使用，更準確地判斷垃圾郵件和“非垃圾”郵件。演算法的資料來來源就是信件的內容。為了更有效率地辨別垃圾郵件和非垃圾郵件，垃圾郵件防護需要一個學習過程。

垃圾郵件防護作為外掛程式被植入以下郵件用戶端：

- Microsoft Office Outlook；
- Microsoft Outlook Express (Windows 郵件)；
- The Bat!；
- Thunderbird。

通過創建白名單和黑名單您可以讓垃圾郵件防護學習從哪些位址發出的郵件應該被認為“非垃圾”郵件，哪些位址發出的郵件應該被認為垃圾郵件。除此之外，垃圾郵件防護還能分析郵件中是否含有被允許和被阻止列表以及色情短語列表中的短語。

垃圾郵件防護可以在伺服器上查看郵件，您可以刪除那些您不想要的郵件。

若要編輯垃圾郵件防護設定：

1. 打開主程序視窗並點擊視窗頂部的設定的接。
2. 在打開視窗的**防護**部分選擇**垃圾郵件防護**。
3. 為您選擇的模組點擊**設定**按鈕。
4. 在組件設定中作必要的更改。

模組操作演算法

垃圾郵件防護的操作主要分兩個階段進行：

1. 第一次的反病毒使用嚴格的過濾標準來進行過濾。這些標準會迅速的確定郵件是否為垃圾郵件。垃圾郵件防護演算法來指定資訊的狀態是否為垃圾郵件，一旦掃描終止，資訊將被轉移到郵件用戶端進行處理。（見步驟1至5所示）。

2. 在下一步驟的演算法中（見步驟6至10所示）。垃圾郵件防護演算法經過之前步驟的精細過濾後，發現郵件符合垃圾郵件的標準，毫無疑問，此類郵件被定義為垃圾郵件。因此，垃圾郵件防護演算法根據資訊符合垃圾郵件的機率來確定其是否為垃圾郵件。

垃圾郵件防護演算法包含如下的步驟：

1. 通過掃描寄信人的位址，來與位址的黑白名單進行匹配。

    - 如果寄信人的位址在白名單，則由其發送的郵件將被認為非垃圾郵件狀態。
    - 如果寄信人的位址在黑名單，則由其發送的郵件將被認為垃圾郵件狀態。

2. 如果使用 Microsoft Exchange 伺服器來發送郵件並禁用了郵件掃描，那麼該郵件將會被指定為非垃圾郵件。

3. 白名單中的訊息都經過線上的分析，如一旦被建立，該郵件會被認為是非垃圾郵件狀態。預設情況會跳過該步驟。

4. 執行郵件分析時將會檢查郵件是否包含禁用詞彙列表中的詞彙。如果在郵件中檢測到這些詞彙將會增加郵件是垃圾郵件的機率。如果累績的機率超過指定的參數值，將會指定該郵件時垃圾郵件或可能的垃圾郵件狀態。執行的郵件分析也會檢查郵件是否包含色情詞彙列表中的詞彙。該步驟預設情況下被跳過。

5. 如果郵件文本包含的位元址包含釣魚或者可疑網址，則指定該郵件為垃圾郵件。

6. 使用啟發式規則來執行郵件分析。如果在郵件中分析出典型的垃圾郵件症狀，那麼它是垃圾郵件的機率增加。

7. 程式使用了GSG技術來分析郵件訊息。垃圾郵件防護會分析附在電子郵件訊息中的圖像。如果在圖像中發現垃圾郵件的相應特徵，該郵件為垃圾郵件的機率將隨之增加。

8. 程式分析附在訊息中的.rtf格式的檔。它掃描附件，檢查它們是否存在垃圾郵件的特徵。在分析完成後，垃圾郵件防護計算郵件是垃圾郵件的機率增加了多少。預設情況下，該技術是被禁用的。

9. 它檢查是否存在典型垃圾郵件的附加特徵。每一個檢測功能都增加了被掃描的郵件是垃圾郵件的機率。

10. 如果進行過垃圾郵件防護學習，將使用貝葉斯技術來掃描郵件。基於在郵件文本中找到的典型垃圾郵件詞彙的頻率來計算郵件是垃圾郵件的機率。

訊息分析確定垃圾郵件的機率。垃圾郵件作者不斷提高它們偽裝垃圾郵件的方法；因此，累計的機率通常達不到指定的參數值。若要確保對郵件訊息有效的過濾，垃圾郵件防護使用如下兩種參數：

- 垃圾郵件機率 – 當郵件被確認為垃圾郵件的時候，都會有一個機率參數。一旦機率小於參數的時候，垃圾郵件防護會將其認為成是疑似垃圾郵件；
- 潛在的垃圾郵件機率 – 當郵件被認為是垃圾郵件的機率大於該參數值，則為潛在的垃圾郵件；而若是機率值小於該參數值，則該郵件不是垃圾郵件。

依靠機率與參數的比較，能很好的區分確認垃圾郵件和潛在的垃圾郵件。基於其當前用的狀態，也會在標籤欄中標注 [！！spam] 或者是[！！Probable spam]。然後，您將通過規則更加明確您用戶端電子郵件的狀態。

廣告橫幅防護

廣告橫幅防護阻止廣告資訊附著在某些網路橫幅上，或者附著在您電腦上安裝的各種程式介面上。

橫幅上的廣告資訊不僅不包含任何有用的資訊，而且還分散和增加了網路流量。廣告橫幅防護使用套裝程式裡的遮罩可以阻止大量已知的普通廣告類型。

大部分普通廣告的遮罩列表由卡巴斯基實驗室的專家編輯，並且被包含在套裝程式裡。如果廣告與列表裡的遮罩相匹配，就會被程式阻止，除非廣告橫幅防護被禁用。如要阻止在標準列表中沒有發現的廣告位址遮罩，將使用啟發式分析。

另外，您可以創建白名單和黑名單來確定允許或阻止什麼樣的廣告。

在安裝好卡巴斯基全功能安全軟體後，廣告橫幅防護模組是被禁用的。

若要編輯反廣告設定：

1. 打開主程序視窗並點擊視窗頂部的**設定**的連結。
2. 在打開視窗的**防護**部分選擇**廣告橫幅防護**模組。
3. 在設定中為您選擇的組件做必要的更改。

家長控制

家長控制是監控使用者訪問網路的程式模組。它的主要目的是限制訪問以下資源：

- 成人網站或者關於色情，武器，違禁藥品，暴力，等等內容的網站。
- 能導致浪費時間（聊天室，遊戲）或浪費金錢（網路商店，網上拍賣）的網站。

應該注意的是，這些網站通常包括大量惡意程式，從這些網站和遊戲網站下載資料會大幅度增加網路流量。

限制使用者訪問網路資源是通過給使用者分配三種使用網路角色來實現的。轉換密碼之後才能轉換角色。

默認時，所有用戶被分為**兒童**角色，擁有最大限制。這些角色與 **Microsoft Windows** 用戶一樣。這種情況下，使用者被賦予依據特定角色訪問網路資源的許可權。

兒童或者**青少年**角色必需有密碼保護。轉換密碼之後才能轉換角色。

每個角色都使用一個事先設定好的限制級別訪問網站。限制級別是一個管理訪問特殊網路資源的設定。

建議您為本程式設定密碼保護，以避免未經授權禁用模組。

在安裝完卡巴斯基全功能安全軟體後，家長控制模組是被禁用的。

若要修改家長控制模組設定，請執行如下步驟

1. 打開主程序視窗並點擊視窗頂部的<u>**設定**</u>的連結。
2. 在打開視窗的**防護**部分選擇**家長控制**模組。
3. 為您選擇的模組點擊**設定**按鈕。
4. 在組件設定中做必要的更改。

掃描我的電腦

掃描我的電腦中的病毒和弱點是確保電腦安全的最重要的任務之一。病毒掃描偵測惡意程式碼的傳播，因為某些原因反病毒程式無法偵測到這些惡意程式碼。弱點掃描偵測軟體弱點，入侵者可能利用這些弱點來傳播惡意物件和訪問私人資訊。

卡巴斯基專家辨別病毒掃描任務的幾種類型：

- **物件掃描**。使用者選擇的物件會被掃描。電腦系統檔案會被掃描。在該任務中您可以為掃描抽取式磁碟設定設定。
- **完全掃描**。整個系統的完全掃描。預設情況下掃描如下的物件：系統記憶體，在啟動時載入的程式，系統備份，郵件資料庫，硬碟，卸載式存放裝置介質和網路硬碟。
- **快速掃描**。掃描作業系統啟動物件。

完全掃描任務和快速掃描任務是指定的任務。推薦您更改這些任務掃描的物件清單。

在指定的區域執行每一個掃描任務並可以根據建立的任務來運行。預設情況下，提供了三個級別。

病毒掃描任務開始後，在 Kaspersky Internet Security 的主視窗的掃描中心部分會顯示它的進度。在偵測到威脅後，程式會執行指定的操作。

當掃描到威脅時，結果會記錄到 Kaspersky Internet Security 的報告中。

更新

保持反病毒資料庫更新是確保電腦得到可靠保護的前提條件。因為每天都會出現新的病毒，木馬，和惡意軟體，有規律的更新應用程式對持續保護您的資訊是很重要的。關於威脅的資訊和處理它們的方法包含在應用程式資料庫中，因此更新資料庫是關鍵之一。

應用程式更新時包括：

- Kaspersky Internet Security 資料庫。
- 儲存在您電腦的反病毒資料庫包含，病毒、網路攻擊的特徵描述和常用的處理它們的方法的資料庫，使您的電腦得到安全保護。本程式的模組提供保護並使用它們來搜索和清除電腦上的有害的物件。每小時資料庫中都會添加新威脅的記錄和處理它們的方法。因此，推薦您定期更新資料庫。 除了 Kaspersky Internet Security 資料庫，網路驅動也會得到更新，使用它來攔截網路流量。
- 程式模組。
- 除了更新資料庫，您還可以更新應用程式模組。模組更新用來修復應用程式的弱點。添加新的功能或改進現有的功能。

Kaspersky Internet Security 的主更新源是卡巴斯基實驗室專門用來更新的更新伺服器。

想要成功地從伺服器下載更新，您的電腦需要連接到網際網路。預設情況下，網際網路連接設定是自動的。如果代理伺服器設定不是自動的，手動為它設定連接設定。

在更新過程中，您電腦上的應用程式模組及資料庫會和更新伺服器上的做比較。如果已經是最新版本的資料庫和應用程式模組，您將看到一個提示視窗，來確認電腦上的保護已經是最新的了。如果電腦和更新伺服器上的資料庫和模組不一樣，應用程式僅下載更新增加的部分。不是下載全部的資料庫和程式模組，這樣顯著地增加了複製檔案的速度和節省了網路流量。

如果資料庫已經過期，更新包可能會很大，從而增加網路流量。

在更新資料庫之前，應用程式為它們建立備份檔案。這份備份檔案可以在您不想要使用最新版本的資料庫時，用來還原資料庫。

您可能需要恢復到上一次更新，例如，如果您更新了資料庫，但是在運行期間它們損壞了。您可以輕鬆還原到之前的版本並稍後再嘗試資料更新。

在程式更新的同時可以執行複製下載的更新到本地的其它位置。該服務允許其它網路電腦在其位置上更新資料庫和程式模組，從而節省互聯網流量。

您也可以設定更新自動啟動。 主程序視窗的**我的更新中心**顯示了應用程式當前資料庫狀態的資訊：

- 威脅類型總數；
- 資料庫狀態（最新的，過期的，或損壞的）。
- 資料庫釋出日期

您可以查看更新報告，報告裡有更新任務執行時發生的事件資訊，您也可以通過點擊病毒活動查看連結。

安全工具中心

確保電腦的安全是一項艱巨的任務，與系統安全相關的資訊，大量及多樣化也增加了在分析和處理的難度。

為了在電腦安全方面能夠提供更方便的方為解決具體的問題，將這一系列的精靈和工具納入 Kaspersky Internet Security 中。

- 虛擬鍵盤，防止對鍵盤上輸入作攔截。
- 建立救援光碟，在遭受病毒攻擊後，如病毒攻擊破壞了作業系統的系統檔，使其無法運行，救援光碟用於恢復系統。
- 調校瀏覽器設定，該精靈從安全角度出發，對 Microsoft Internet Explorer 瀏覽器的設定進行分析。
- Windows 設定疑難排解，恢復被惡意軟體損壞的設定。
- 清理您的活動記錄，搜索和清除系統中使用者活動的跟蹤。
- 網路資料分析，攔截網路資料，並顯示其詳細資訊。
- 家長控制，為兒童和青少年提供了健康的上網環境。

報告

報告中記錄了應用程式每個模組的操作、每次病毒掃描的執行和應用程式的更新。

在報告中您可以選擇以下操作：

- 選擇您需要查看相關報告的模組和任務；
- 管理資料分組並在螢幕上顯示資料；
- 根據 Kaspersky Internet Security 建立一個計畫將提醒您報告就緒；
- 選擇您想要建立報告的事件類型；
- 選擇統計資訊在螢幕上顯示的方式；
- 以檔來保存報告；
- 指定過濾條件；
- 設定搜索發生在系統中的事件並根據程式來處理。

通知

當事件在應用程式運行時發生，螢幕上會彈出相關的資訊。根據事件的安全危急程度，您可能會收到以下的通知類型：

- **警報**。發生一件嚴重的事件，例如，在系統中偵測到一個惡意軟體物件或危險行為。您應該立即決定程式如何回應。這種類型的通知視窗顯示為紅色。
- **警告**。發生一件潛在的危險事件。例如，在系統中偵測到潛在被感染的物件或可疑行為。根據您判斷的事件危險程度，來指示程式執行操作。這種類型的通知視窗顯示為黃色。
- **信息**。該通知告訴您非緊要事件的資訊。這種類型的通知視窗顯示為綠色。

通知視窗由四個部分組成：

1. 窗口描述。通知視窗標題包含一個事件的概述，例如：許可權請求，可疑行為，新的網路連接，警報，病毒。
2. 事件描述。事件描述區域顯示了原因的詳細資訊：引起事件發生的程式名，偵測到的威脅名稱，偵測到的網路連接的設定等。
3. 操作選擇區域。這一部分您可以為該事件選擇一個可用的操作。建議的操作選項取決於事件的類型，例如：**清除**，**刪除**，**略過** - 如果偵測到一個病毒，**允許**，**中止** - 如果一個程式請求執行潛在有害的操作的許可權。卡巴斯基實驗室專家推薦的操作將以粗體字的形式顯示。

   如果您選擇了**允許**或者**中止**，您可以在接下來打開的視窗中選擇操作應用模式。對於**允許**操作您可以選擇一個如下的模式：

- <u>總是允許</u>。需要允許程式更改訪問系統資源的規則，請選擇該選項。
- <u>現在允許</u>。應用的時間為從對話開始直到對話被關閉或重新啟動。
- <u>添加到受信任</u>。選擇該項來移動程式到受信任組別。

對阻止的操作您可以選擇一個如下的方式：

- <u>總是阻止</u>。需要阻止程式更改訪問系統資源的規則，請選擇該選項。

- <u>現在</u>中止。在程式當前對話期間應用選擇的操作到偵測到的所有類似的事件，請選擇該項。應用的時間為從對話開始直到對話被關閉或者重啟。

- 中止。選擇該項來終止程式的運行。

  附加操作選擇區域。使用該部分您可以選擇一個附加操作：

- <u>添加到排除</u>。如果您確定偵測到的物件是無害的，我們推薦當您在使用該物件時添加它到信任區域。

- <u>套用到所有物件</u>。選中該方塊，強行將指定的操作應用到在類似情況下有相同狀態的所有物件。

確認 Kaspersky Internet Security 設定

安裝和設定完程式後，您可以使用一個測試"病毒"和其變種來檢查應用程式的設定是否正確。您還可以針對每一個保護模組和協定進行獨立的測試。

測試病毒和變種：EICAR 和它的變種

該測試病毒是由(歐洲電腦反病毒研究中心)專門設計用來測試反病毒產品。 該測試病毒不是一個真正的病毒。因為它不包含會損害電腦的代碼。然而，大部分的反病毒產品製造廠商鑒定該檔是一個病毒。

不要使用真正的病毒來測試反病毒產品的運行！

您可以從 EICAR 的官方網站下載這個測試"病毒"：
http://www.eicar.org/anti_virus_test_file.htm.

在下載該檔之前，您需要禁用反病毒保護，因為應用程式會鑒別和處理檔 anti_virus_test_file.htm 為一個通過 HTTP 協定傳送的被感染物件。在下載完該測試"病毒"後，不要忘記立即啟用反病毒保護。

應用程式鑒定從**EICAR**網站下載的檔是一個包含病毒的被感染物件。如果病毒不能被清除，並對這個物件執行指定的操作。

您也可以使用標準測試病毒的變種來檢驗應用程式的運行。方法是通過添加以下首碼之一（見下表）到標準病毒來更改其內容。想要建立測試病毒的變種，您可以使用任意的文本或超文字編輯器。例如 **Microsoft Notepad,UltraEdit32**，等。

只有反病毒資料庫最後更新時間在2003年10月24日或這個日期之後（2003年10月累計的更新）。您才可以使用 EICAR 病毒變種來偵測反病毒應用程式運行的正確性。

在下表中，第一列包含首碼，用來添加到標準測試"病毒"字串的開頭。第二列列出了反病毒基於掃描結果給物件賦予的所有可能的狀態值。第三列包含關於在指定狀態下處理物件的資訊。請注意對物件執行的操作由程式中設定的值來確定。

在您對測試病毒添加完首碼後,用不同名字保存新檔,例如：eicar_dele.com .給所有變種"病毒"指定類似的名字。

測試HTTP流量保護

Ø 若要驗證對通過 *HTTP* 協定傳輸的資料流程中的病毒的偵測功能,請執行如下操作：
從官方網站下載一個測試"病毒"，網址為：
http://www.eicar.org/anti_virus_test_file.htm.

當您嘗試下載測試"病毒"時，卡巴斯基反病毒安全軟體將會偵測到該物件，將其識別為無法被清除的被感染對象，並且將執行在HTTP流量保護設定中針對該類物件相應的操作.預設情況下，當您從該網站下載測試"病毒"時,網路連接將被終止，瀏覽器將顯示一條資訊來通知使用者，該物件被測試"病毒"EICAR-Test-File感染。

測試SMTP流量保護

為了偵測使用SMTP協定傳輸的資料中有無病毒，您必須使用一個利用該協定傳輸資料的電子郵件系統。

我們建議您測試反病毒如何處理出站的電子郵件，包括郵件正文和附件。若要測試偵測正文中的病毒，將標準的測試"病毒"或者修改過的"病毒"複製到郵件中。

Ø 測試步驟：

1. 使用安裝在電腦上的郵件用戶端建立一封普通文本格式的郵件。
   - 如果以RTF或HTML格式建立的話，含有測試病毒的郵件不會被掃描 ！
2. 將標準的或修改過的測試"病毒"複製到郵件的開頭，或者附加一個含有測試"病毒"的檔。
3. 發送郵件給管理員。

應用程式將偵測物件，判定為受感染的，並阻止該郵件。

確認檔反病毒設定

Ø 若要驗證檔反病毒的設定是否正確,請執行如下操作：

1. 在磁片上建立一個資料夾，將從EICAR組織官方網站 (http://www.eicar.org/anti_virus_test_file.htm) 下載的測試“病毒”及您建立的所有病毒的變種複製至該資料夾。

2. 允許記錄所有事件，所以報告檔保留了關於被破壞物件的資料和因為錯誤無法掃描的物件。

3. 運行測試“病毒”或其變種。

檔反病毒將截斷對檔的調用掃描檔。並且執行設定中指定的操作。通過選擇在偵測到物件時的不同操作。您將可以對模組的操作進行全盤檢查。

您可以在關於模組的操作的報告中查看關於檔反病毒模組運行結果的資訊。

解決問題

如果應用程式使用時出現任何問題，首先確認問題的解決方法是否在説明系統或者在卡巴斯基實驗室知識庫中。知識庫是技術支援網站的單獨部分，有卡巴斯基實驗室產品推薦和常見問題解答。儘量使用這個資源來找到您問題的答案或者解決辦法。

Ø 若要使用知識庫：

1. 打開主程序視窗。

2. 在視窗底部點擊技術支援的連結。

3. 在打開的支援視窗點擊知識庫的連結。

另外一個程式應用資訊源是 Kaspersky 論壇。這也是技術支援網站的一個單獨區域，且包含使用者疑問、回饋和請求。您能查看主題，留下回饋意見或者找到問題的答案。

Ø 打開使用者論壇的步驟：

1. 打開主程序視窗。

2. 在視窗底部點擊技術支援的連結。

3. 在打開的技術支援視窗點擊支援工具的連結。

如果您在幫助或論壇中未找到解決方法，我們建議您聯繫技術支援。

建立系統狀態報告

當卡巴斯基實驗室的專家在幫您解決電腦問題時,可能要求一個系統狀態報告.這個報告包含了關於運行的進程、下載的模組和驅動、Microsoft Internet Explorer 和 Microsoft Windows Explorer 外掛程式、打開的埠、偵測到的可疑物件等詳細資訊。

當建立系統狀態報告時，不會收集使用者私人資訊。

Ø 若要建立一份系統狀態報告:

1. 打開主程序視窗。

2. 在視窗底部點擊技術支援的連結。

3. 在打開的技術支援視窗點擊支援工具的連結。

4. 在打開的技術支援服務資訊視窗，點擊建立系統狀態報告按鈕。

建立的系統狀態連結是以 *html* 和 *xml* 格式保存在壓縮包 *sysinfo.zip* 中的。一旦收集資訊過程結束，您可以查看報告。

Ø 若要查看報告:

1. 打開主程序視窗。

2. 在打開的技術支援視窗點擊支援工具的連結。

3. 在打開的技術支援服務資訊視窗點擊查看按鈕。

4. 打開包含報告檔sysinfo.zip壓縮包

建立跟蹤文件

在卡巴斯基反病毒安全軟體安裝後。在作業系統或個別的程式運行時可能會發生一些故障。很可能是卡巴斯基反病毒安全軟體和您電腦上安裝的軟體或電腦模組的驅動發生了衝突。您需要建立一份跟蹤檔。以方便卡巴斯基實驗室的專家來順利地解決您的問題。

Ø 若要建立一份跟蹤文件:

1. 打開主程序視窗。

2. 在視窗的底部點擊的支援連結。

3. 在打開的技術支援視窗點擊支援工具的連結。

4. 在打開的技術支援服務資訊視窗的跟蹤部分使用下拉式功能表來選擇跟蹤等級。跟蹤等級由技術支援專家來定義。如果從技術支援處沒有可用的提示，那麼推薦使用等級標準（**500**）

5. 點擊啟用按鈕來啟動跟蹤程式。

6. 重現情形來使問題發生。

7. 選擇禁用按鈕，停止跟蹤。

您可以切換到上傳跟蹤結果到卡巴斯基實驗室伺服器。

發送資料檔案

在您建立完跟蹤檔和系統狀態報告後，您將需要發送它們到卡巴斯基實驗室技術支援服務專家。

您將需要輸入要求的編號來上傳資料檔案到技術支援.如果申請是啟動的。在技術支援網站上您的個人專區中的這個號碼是有用的。

Ø 想要上傳資料檔案到技術支援服務伺服器：

1. 打開主程序視窗。
2. 在視窗底部點擊支援的連結。
3. 在打開的支援視窗點擊支援工具的連結。
4. 在打開的技術支援服務資訊視窗的操作部分，點擊上傳技術支援服務資訊到伺服器按鈕。
5. 選中您想要發送到技術支援服務的跟蹤檔的核取方塊，然後選擇發送按鈕。
6. 輸入請求編號視窗輸入號碼。

選擇了的跟蹤檔會被壓縮並發送到技術支援服務伺服器。 如果不能聯繫技術支援，您可以在您的電腦上保存資料檔案。

Ø 想要保存資料檔案到硬碟中：

1. 打開主程序視窗。
2. 在視窗底部點擊支援的連結。
3. 在打開的支援視窗點擊支援工具的連結。
4. 在打開的技術支援服務資訊視窗的操作部分點擊將技術支援服務資訊上傳到伺服器按鈕。\
5. 選中您想要發送到技術支援服務的跟蹤檔的核取方塊，然後選擇發送按鈕。
6. 在打開的輸入要求編號視窗點擊取消按鈕，並確認保存檔到磁片。
7. 在打開的視窗置頂壓縮包名稱。

.稍後您可以在個人專區的幫助下發送保存的檔到技術支援。

執行AVZ腳本

卡巴斯基實驗室專家將基於追蹤檔和系統狀態報告來分析您的電腦。分析結果通常是一串很長的操作序列，目的是消除偵測到的問題。 使用AVZ腳本來簡化過程。AVZ腳本是一系列允許進行以下操作的指令：修改註冊表、隔離檔、查找能隔離相關檔的類別，禁止使用者模式和核心模式的阻止者等。 應用套裝程式含一個AVZ腳本執行精靈來運行腳本。這個精靈包含一系列視窗，使用上一步和下一步來操作。一旦完成，使用完成鍵來關閉精靈.用取消鍵來取消精靈。 卡巴斯基實驗室專家不建議您更改腳本內容。如果在腳本執行過程中出現問題,請聯繫技術支持。

Ø 若要啟動精靈：

1. 打開主視窗程式。
2. 在視窗底部點擊支援的連結。
3. 在打開的支援視窗點擊支援工具的連結。
4. 在打開的技術支援服務資訊視窗點擊執行 **AVZ** 腳本按鈕。

成功執行腳本後，精靈會關閉。如果在腳本執行過程中發生了一個錯誤，精靈將顯示相應的錯誤資訊。

Kaspersky Security Network 資料收集聲明

A. 簡介

在您繼續使用我們的服務或軟體之前請仔細閱讀該文檔，其中包含您需要瞭解的重要資訊。如果繼續使用卡巴斯基實驗室軟體和服務，您將被視為已經接受了卡巴斯基實驗室資料收集聲明。我們保留隨時修改該聲明的權利，並會將更改公佈在網頁中。在您決定接受條款之前，請檢查最後的修改日期，因為在您最後一次審閱後這些條款有可能被修改。在資料收集聲明更新後，您對卡巴斯基實驗室服務的任 何一部分的使用，都等同於您已經接受已更改的聲明。

卡巴斯基實驗室和他的分支機構（通稱為卡巴斯基實驗室）建立了這份資料收集聲明，目的是告知和公開 Kaspersky Internet Security 和 Kaspersky Internet Security 資料收集和分發方法。

卡巴斯基實驗室承諾 卡巴斯基實驗室鄭重承諾將對我們使用者提供最優質的服務，尤其尊重您對資料收集的關注。我們理解您可能對 Kaspersky Security Network 如何收集和使用資料有疑問，因此我們準備了這份聲明以告知您運行 Kaspersky Security Network（“資料收集聲明”或者“聲明”）的資料收集原理。

這份資料收集聲明中包含很多常規和技術的詳細資訊，目的是告訴使用者我們是 如何收集和使用資料的。我們針對主要的方法和範圍編制了這份資料收集聲明。目 的是您可以快速查閱自己感興趣的內容。我們的主旨是滿足您的需要和期望－包括保護您的資料收集。 如果您在查閱完資料收集聲明後有任何疑問， 請送電子郵件到 info@kaspersky.com.hk。

什麼是 Kaspersky Security Network ？

Kaspersky Security Network 服務將說明全球的卡巴斯基實驗室安全產品使用者，更加方便地識別威脅並減少抵禦針對您電腦的最新安全風險所需要的時間。為了識別新威脅和它們的來源，並幫助提高使用者的安全性和產品功能，Kaspersky Security Network 收集選定的安全和應用程式資料（有關針對電腦的潛在威脅）並把它們提交到卡巴斯基實驗室進行分析。這些資訊不包含使用者個人身份資訊，卡巴斯基實驗室只會利用這些資料來加強其安全產品的保護能力，並且提供更先進的解決方案以防禦惡意威脅和病毒，不會作其它用途。如果使用者個人資訊意外傳送，卡巴斯基實驗室將根據本資料收集聲明來妥善保護這些資料。

通過加入 Kaspersky Security Network，您和其他來自全球的卡巴斯基實驗室安全產品的使用者就構成了一個安全的互聯網環境。

法律相關

Kaspersky Security Network 需要遵從于一些管轄區的法律，因為它的服務會用於不同的管轄區，包括中華人民共和國和香港特別行政區。當法律要求或者我們相信是為了協助

調查或保護卡巴斯基實驗室的客人，訪客，合作夥伴，或者財產及其他人免受危害時，卡巴斯基實驗室會在不經過個人允許的情況下透露這些資訊 。如上所述，Kaspersky Security Network 收集資料和資訊的相關法律會因國家不同而有所改變。 當開始收集上述資訊，分享這些資料，特別是用於商業開發用途時，Kaspersky Security Network 會及時通知使用者，並允許這些網路使用者線上選擇加入（中華人民共和國，香港特別行政區，和其他需要選擇加入程式的國家）或者選擇退出（所有其他國家）將這些資料用於商業用途或傳遞這些資料給協力廠商。 卡巴斯基實驗室會根據執法或司法機關要求，提供一些個人身份資訊給相關的政府部門。若執法或司法機關要求，我們會在收到適當的檔後提供這些資訊。為了保護個人的財產，健康和安全，當法律許可時，卡巴斯基實驗室也可以提供這些資訊。 個人資訊保護成員國當局的聲明將依照中華人民共和國和香港特別行政區的法律生效。關聲明的資訊內容，可以從 Kaspersky Security Network 服務上獲得。

B. 收集資訊

我們收集的資料 Kaspersky Security Network 服務將收集並提交針對您電腦的潛在安全威脅資料，這些資料分為核心資料和擴展資料，這些收集到的資料包括： 核心資料 關於電腦的硬體和軟體資訊，包括作業系統和服務升級包，內核對象，驅動程式，服務，WEB瀏覽器，印表機，Windows 瀏覽器，下載的程式檔， 活動安裝元素 ，控制台，主機和註冊表 ，IP地址，瀏覽器類型，e-mail 用戶端和卡巴斯基實驗室產品的版本號，這些都不涉及個人身份資訊； 卡巴斯基實驗室產品生成的唯一ID，該ID不包含任何個人資訊，用來識別個人電腦而不是使用者； 有關您電腦反病毒保護的狀態資訊，一些檔和可疑物件資料（例如，病 毒名稱，偵測時間/日期，受感染檔的名稱/路徑和大小，IP 位址和網路攻擊的埠，可疑惡意程式的名稱）。這些收集的資料不包括個人身份資訊。 擴展資料 使用者下載的具有數位簽章的程式資訊（URL，檔大小， 簽名者名稱）； 可執行程式的資訊（大小，屬性，建立日期，PE頭資訊，區域，名稱，位置和使用的壓縮工具）。 傳輸和存儲資料的安全

卡巴斯基實驗室致力於保證資訊安全，收集到的資訊將被存儲在受到限制和控制訪問的伺服器上。卡巴斯基實驗室運行著由達到行業標準的防火牆和密碼保護系統保護的安全資料網路。卡巴斯基實驗室採用了多種安全技術和程式來防護收集到的資料免受未經授權的訪問，使用或洩露的威脅。我們的安全性原則是定期檢查和加強的，僅獲得授權的個人能訪問收集的資料。卡巴斯基實驗室採取措施保證您的資訊如本聲明所述的一樣安全。遺憾的是，我們不能保證所有的資料安全。因此，儘管我們

將努力保護您的資料，但我們仍不能保證您傳送給我們的任何資料或者從我們的產品或服務傳送的任何資料是安全的，這些服務包括但不限於 Kaspersky Security Network，您使用這些服務可能產生的風險需要自己承擔。 收集來的資料將被傳送到卡巴斯基實驗室伺服器，卡巴斯基實驗室已經採取措施保護這些資料安全，在傳送時，我們把收集的資訊視為機密資訊並提供相應的保護級別；它會遵守我們機密資料使用的安全程式和企業策略。按照行業慣例，收集到的資訊傳送到卡巴斯基實驗室後，將被存儲在具有物理和電子保密措施保護的伺服器上，這些措施包括密碼/登錄程式和專為阻止那些來自卡巴斯基實驗室之外的未 經授權的訪問而設計的防火牆。本聲明涉及的 Kaspersky Security Network 收集的資料，將會 在中華人民共和國和香港特別行政區，或者在其他有卡巴斯基實驗室商業行為的管轄區或國家進行處理和儲存。所有卡巴斯基實驗室的員工都知道我們的安全性原則。 您的資料僅會被那些需要用它來完成工作的員工使用。任何存儲的資料都不包含個人身份資訊。卡巴斯基實驗室不會將 Kaspersky Security Network存儲的資料與任何其他資料，連絡人清單，或者由卡巴斯基實驗室收集來為宣傳或做其他用途的訂閱資訊相結合。

C. 使用收集到的資料如何使用您的資訊？

卡巴斯基實驗室收集這些資料是為了分析和識別潛在的安全威脅，提高卡巴斯基實驗室產品的偵測惡意行為、欺詐網站、流氓軟體和其它類型的互聯網威脅的能力，以便為用戶提供更高水準的保護。 向協力廠商透露資訊 若執法人員要求或法律允許，作為對法律程式或者法院傳票的回應，或者如果我們相信這樣做是為了遵守法律，法規或其他法律程式或政府要求，卡巴斯基實驗室可以透露任何收集的資訊。當我們有理由相信透露這些資訊是為了查明，聯繫或針對您提出訴訟所必需的，當您可能違反了本聲明、您與本公司的協議條款時，或者保護我們用戶和公眾的安全，或是針對簽定了保密協議與授權授權合約的某些特定的協力廠商（幫助我們開發，運作和維護 Kaspersky Security Network），卡巴斯基實驗室也可以透露這些資訊。為了宣傳，偵測及預防互聯網安全風險，卡巴斯基實驗室可與研究組織和其他安全軟體廠商共用某些資訊，還可以利用收集來的統計資料，跟蹤或發表關於安全風險趨勢的報告。 您的選擇加入 Kaspersky Security Network 是可以選擇的。您可以通過卡巴斯基實驗室產品選項的回饋設定，隨時啟動或者禁止 Kaspersky Security Network 服務。然而，如果您拒絕提供要求的資料或資料，我們可能無法向您提供基於這些資料資料的服務。一旦卡巴斯基實驗室產品服務週期結束，卡巴斯基實驗室軟體的某些功能還能繼續工作，但是資訊將不再能自動發送到卡巴斯基實驗室。 我們也保留發送少量的警告資訊給使用者的權利，這些資訊用於通知他們先前簽署服務的某些變更可能對他們使用我們的服務產生影響。我們也保留與您聯繫的權 利，在不得不作為法律程式的一部分，或者有任何違反許可，授權和購買協議的行為發生時，我們將會與您聯繫。 卡巴斯基實驗室保留與您聯繫的權利，因為在一些情況下，我們需要聯繫您（如 果法律需要或是由於對您十分重要的事件）。我們不會使用這些權利來向您推廣新 的或現存的服務，如果您要求我們不這樣做，我們不會給您發送這種類型的資訊 。

D．資料收集相關的查詢和投訴

卡巴斯基實驗室以最大的尊重與關注，來處理使用者的資料收集。如果您認為本聲明中關於您的資訊資料有不符之處，或者您有其它相關的諮詢或關注，您可以通過電子郵件聯繫卡巴斯基實驗室，郵寄地址：info@kaspersky.com.hk。

在您的郵件當中，請盡可能詳細描述您的問題。我們將及時調查您的問題或投訴。

個人資訊的提供是自願的。使用者可以隨時通過卡巴斯基產品“回饋”中禁用資料收集這一功能。

卡巴斯基實驗室

卡巴斯基實驗室成立於1997年。今天，它已經成為一家領先的國際資訊安全軟體提供商。卡巴斯基實驗室研發、生產和銷售廣泛的資訊安全解決方案，包括：反病毒、垃圾郵件防護和反駭客系統。

卡巴斯基實驗室的總部設在俄羅斯莫斯科，並在英國、法國、德國、荷蘭、波蘭、日本、中國、韓國、羅馬尼亞以及美國設有分支機構。最近我們的歐洲反病毒研究中心也在法國成立了。卡巴斯基實驗室的全球合作夥伴超過500家，網路覆蓋全球各地。

目前，卡巴斯基實驗室由超過千名的高素質員工組成，其中10位具有MBA學位，還有16位具有博士學位。卡巴斯基實驗室的眾多反病毒領域專家同時也是電腦病毒研究組織(CARO)的成員。

卡巴斯基實驗室的專家在過去14年與電腦病毒的不懈鬥爭中，積累了大量的業內領先經驗和知識，這也是我們公司最大的財富。對電腦病毒的透徹分析，使得我們公司的專家能夠準確地預見惡意軟體的發展趨勢，並給我們用戶提供針對最新威脅的最及時保護。該優勢為卡巴斯基實驗室的產品和服務鑄就了穩固的根基。同時，這也使我們能夠隨時為我們的用戶提供領先一步的反病毒保護。

公司員工年復一年的辛勤工作，使卡巴斯基實驗室成為了頂尖的反病毒軟體研發提供商之一，我們在行業內率先開發出了大量的反病毒軟體標準。我們公司的旗幟產品，卡巴斯基反病毒，能夠為幾乎所有的電腦提供可靠的反病毒保護，這些電腦括：工作站、檔案伺服器、郵件系統、防火牆、閘道和掌上型電腦。我們方便易用的集中管理工具能夠為企業網路和各類電腦提供最大化地自動反病毒保護。許多知名的業內廠商都在他們的產品中內嵌了卡巴斯基反病毒的內核程式。他們包括：Nokia ICG (美國)， F-Secure (芬蘭)， Aladdin (以色列)，Sybari (美國)，G Data (德國)，Deerfield (美國)，Alt-N (美國)，Microworld (印度) 和 BorderWare (加拿大)。 卡巴斯基實驗室的客戶將享受周到的服務，我們每小時更新資料庫。公司給客戶提供了24小時的免費技術支援服務，並用多種語言為全世界客戶服務。

最終用戶授權授權合約

標準最終用戶授權授權合約 所有用戶（含自然人、法人或其它組織）請注意：以下是卡巴斯基實驗室(以下稱為“卡巴斯基實驗室”)編制的 Kaspersky Internet Security 2009 (以下簡稱為“軟體”)的授權許可的法律協議(以下簡稱為“ 協議”)，在繼續安裝及開始使用本軟體前，務請仔細閱讀。

若您是通過國際互聯網，選擇點擊“接受”按鈕購得本軟體，則表明您已同意受此協議約束，並成為此協議中的一方。若您不同意本協議的所有條款，請按一下表明您不接受本協定條款的按鈕，且不要安裝本軟體。

若您是以物理介質的形式購得本軟體，且已打開光碟的封套，則表明您已同意受此協議的約束。 此處所述“軟體”包含由卡巴斯基實驗室提供給您的軟體啟動檔(包括“啟動碼”及“授權許可檔”)。

1. 授權許可。在您已支付相應的許可費用及同意本協議條款和條件的前提下，卡巴斯基實驗室在此授予您以非獨占的、非轉讓的方式在本協定的條款下僅為自己內部事務目的而使用本軟體指定版本的副本以及附隨文檔(以下簡稱“文檔”)的權利。

1.1 使用。 本協定僅授權您將本軟體用於保護您所購買的啟動碼或授權許可檔（key 檔）中所指定的數量的電腦作業系統(以下簡稱為“設備”)，即 在啟動碼或授權許可檔指定的數量的電腦、工作站、終端機、掌上型電腦或其它數位電子儀器（每 個虛擬機器，虛擬系統也算作一個獨立的電腦系統）上安裝、使用 、顯示、運行（“運行”）本“軟體 ” 的指定的數量的副本，一份“軟體”啟動碼或授權許可檔不得 在超出其所指定的數量的設備上共同或同時使用。

1.1.1 當軟體被載入上述設備的記憶體(即隨機記憶體或RAM)或安裝到固定記憶體(如硬碟、光碟、或其它存放裝置)中時，即視軟體在您的設備上“使用”。為本軟體的合法使用及備份的目的，本授權許可您製作本軟體 1 份備份，該備份必須包含本軟體所有權的全部公告。您負責保存本軟 件和文檔的所有備份(包 括數量和備份地點)的記錄，並負責採取一切適當的預防措施，以避免本軟體被未經授權地複製或使用。但如果您已經將軟體裝入硬碟，您應該將原盤作為備份而不能再複製。在您喪失該備份的所有權時，您應該負責將備份複製品銷毀。

1.1.2 本軟體致力於保護您的設備免受病毒的侵擾。這些病毒的相應特徵資訊已包含在卡巴斯基實驗室升級伺服器上的反病毒資料庫中。

1.1.3 如果您要將安裝有本軟體的設備出售，請確保在售出前將本軟體從設備上完全刪除。

1.1.4 您不能通過反編譯、反向工程、反彙編等手段將本軟體的任何部分破譯為人類可讀的形式，也不能許可任何協力廠商（含自然人、法人或其它組織）這樣做。為獲得使本軟體與獨立建立的電腦程式的協同操作所需的介面資訊，在提出請求並

支付了合理的費用後，由卡巴斯基實驗室提供上述相關資訊。如果卡巴斯基實驗室通知您，由於任何原因(包括但不限於成本)不能提供這些資訊，您才被許可在法律 允許的反向工程或反編譯的範圍內獲得軟體的互用性資訊。

1.1. 5 在獲得明確的書面許可之前，您不能對本軟體進行錯誤修正，或修改、改編、翻譯本軟體，不能建立本軟體的衍生工程，也無權為任何協力廠商（含自然人、法人或其它組織）或允許任何協力廠商（含自然人、法人或其它組織）複製本軟體。

1.1.6 您不能向任何協力廠商（含自然人、法人或其它組織）租用 、出租或借出本軟體，也不應將您獲得的授權許可轉讓或向任何協力廠商（含自然人、法人或其它組織）二次授權。 1.1.7 您不能使用本程式製作自動、半自動或手動的任何可以生 成反病毒資料庫的工具、進行病毒偵測的程式和其他的用於偵測惡意程式碼和資料的代碼及資料。本軟體作為一個整體，您不得將本軟體分解在不同的電腦上使用或嵌入其他軟體系統。

1.1.8 卡巴斯基實驗室可以要求使用者安裝本軟體的最新版本(包括最新的版本和最新的程式修正包)。

1.1.9 終端使用者必須保存好合法購得的 卡巴斯基產品的資格證明，包括產品光碟、使用者手冊、啟動碼或授權許可檔、及購買憑證等。這些在您享受服務、重新安裝、及產品升級時是不可複得且不可或缺的。在您無法提供合法購得卡巴斯基產品的資格證明時，卡巴斯基實驗室有權拒絕為您提供服務。

1.1.10 您有權為卡巴斯基實驗室提供關於您電腦的潛在威脅和弱點的資訊（詳細資訊，請查閱資料收集聲明）。這些資訊用來提高卡巴斯基實驗室的產品性能。

1.1.11 為了達到 1.1.10 條款中規定的目標，軟體將自動收集在電腦上執行的檔資訊，並發送到卡巴斯基實驗室。 2. 支持。 2.1 卡巴斯基實驗室將在合法的授權許可(授權許可文件或啟動碼)的有效期內，向您提供 24 小時*365 天技術支援服務。合法的授權許可有效期從您第一次合法正式激 活本程式之時算起，但您必須同時具備下列條件：

2.1.1 已支付軟體及支援費用。

2.1.2 完成終端使用者享受卡巴斯基實驗室 的技術支援服務所需的資 格認定附加註冊， 以建立給予您技術服務的身份檔案。在啟動本軟體和/或獲得終端使用者 ID 後，獲得 終端使用者享有的技術支援服務。

2.2 卡巴斯基實驗室具有絕對的獨立判斷權，以決定您是否滿足享受上述技術支援服務的條件。卡巴斯基實驗室有權在必要時向終端使用者要求附加的註冊以便檢驗與技術支援服務相關的資訊。一般情況下，您需要按年度和當時的服務費用標準支付下一年度的產品和技術支援服務費用，並重新成功完成技術支援服務預約表，以保 證軟體的升級和工作正常連續，享受的技術支援服務正常連續。

2.3 在合法的授權許可的有效期內，向 Kaspersky Internet Security 2009 使用者提供的技術支援服務包括：

(a) 反病毒資料庫的常規升級；
(b) 網路攻擊資料庫更新；
(c) 垃圾郵件防護資料庫更新；
(d) 免費的同類型軟體之間升級，包括同類型軟體的版本升級；
(e) 由銷售商和/或分銷商提供的、通過互聯網和熱線電話給予的技術支援；
(f) 24 小時迴圈的病毒偵測與殺毒更新；

2.4 在您的電腦設備中安裝了最新版本軟體（包括程式修正包）的情況下，技術支援服務才可生效，最新的軟體及程式修正包可在卡巴斯基官方中文網站（www.kaspersky.com.hk）或卡巴斯基指定的官方下載網站下載。

3. 所有權。本軟體受俄羅斯聯邦版權法、中華人民共和國著作權法和相關法律法規 保護。卡巴斯基實驗室及其供應商擁有並保留本軟體的所有權利、名稱和利益，包括所有著作權、版權、專利權、商標專有權和其它智慧財產權。您在合法購買本軟體 並獲得合法使用的授權許可後，可在一定時限內持有、安裝及使用本軟體，但並未 獲得本軟體的任何智慧財產權。除本協定明確闡述的內容外，您未獲得與本軟體相關的任何其它權利。

4. 保密。您同意本軟體 和相關文檔(包括各程 序的特殊設計、結構 及啟動碼或授權許可檔)屬於卡巴斯基實驗室的專有機密資訊。未經卡巴斯基實驗室事先書面同意，您不能以任何形式向任何協力廠商洩露、提供這些機密資訊或使這些機密資訊可被獲得。您應採取適當的安全措施以保護這些機密資訊，對保障啟動碼或授權許可檔的安全採用的最佳方式沒有限制。

5. 有限擔保。

5.1 卡巴斯基實驗室承諾，本軟體首次下載或合法安裝後半年內，遵循本產品文檔 指示進行正確操作，實現文檔中描述的功能。

5.2 您同意自行承擔選擇本軟體來滿足您的需求的全部責任。卡巴斯基實驗室不擔保本軟體和/或文檔適合您的全部需求。由於影響軟 件正常運行的因素具有複雜性、進行性和不可預測等特徵，因此卡巴斯基實驗室不擔保任何使用都不會間斷、或運行毫無差錯、或資料毫無損失。

5.3 卡巴斯基實驗室不擔保本軟體可識別所有已知或未知的病毒，也不擔保本軟體不會偶爾出現病毒誤報。

5.4 卡巴斯基實驗室不擔保本軟體在授權許可檔過期後仍可對設備提供保護。

5.5 在合法的授權許可的有效期內，如果將出現與5.1款不符的情況報告給卡巴斯基實驗室或其指定的分銷商，卡巴斯基實驗室的全部責任及對您的賠償由卡巴斯基

實驗室在修復、更換本軟體或退還本軟體購買款選項中做出選擇。您應當向軟體供 應商提供所有合理和必要的資訊，以協助解決其它問題。

5.6 在 5.1中的擔保不適用於下列情況：

(a) 未經卡巴斯基實驗室同意，用戶直接或間接地對本軟體作了修改。
(b) 用戶用不恰當的操作方式使用本軟體。
(c) 用戶沒有遵照本授權授權合約使用本軟體。

5.7 本協定中陳述的擔保和條件取代所有其它有關提供、假設提供、無法提供或延遲提供本軟體或文檔的條件、擔保或期限。除本條第5.4 款外，被取代的資訊或許已在卡巴 斯基實 驗室與您之間的暗示或合併加入此授權授權合約或任何間接合約之間發生作用。無論是法規、習慣法或其它律法，都據此排除(包括但不限於暗示的條件、擔保或其它諸如滿意的品質、適用性及合理的使用技巧等條款)。

6. 有限責任。

6.1 本協議不排除或限制卡巴斯基實驗室的下列責任：

(a) 欺詐性民事侵權行為。
(b) 因違背習慣法的關照責任或因任何疏忽而違背本協議的某項條款導致的死亡或者人身傷害。
(c) 法律規定不得排除的任何責任。

6.2 在 6.1 款條件下，供應商對下列任何損失或損害(無論這些損失或損害是預見的、 可預見的、已知的或其它任何情況)不承擔任何責任(無論在合同、民事侵權行為、 復原或其它方面)：

(a) 收入損失。
(b) 實際或預期利潤的損失(包括合同利潤損失)。
(c) 資金使用的損失。
(d) 預期儲蓄的損失。
(e) 商業交易的損失。
(f) 機會喪失。
(g) 商譽損失。
(h) 名譽損失。
(i) 資料的丟失、損壞或訛誤。
(j) 無論任何原因引起的任何間接或繼發的損失或損害(包括為避免疑惑，從本條第6.2 款(a)段到第 6.2 款(i)段中列明的損失或損害的種類)。

6.3 根據第 6.1 款，與提供本軟體相關的卡巴斯基實驗室的全部責任(無論在合同、 民事侵權行為、復原或其它方面)在任何情況下不超過您為本軟體所支付的費用。

7. 本協議的解釋服從中華人民共和國的法律。當事人可據此向中華人民共和國的法 院提起訴訟。卡巴斯基實驗室保留作為原告時在中華人民共和國法律管轄的任何法 院提起訴訟的權利。 8. 對本協議的理解。

8.1 本協定包含了雙方就所述軟體的完整諒解，並代替您與卡巴斯基實驗室之間所 有和任何先前的、無論口頭的還是書面的諒解、擔保和承諾。這些諒解、擔保和承 諾或許先於本協議，由我們或我們的代表在商談中以任何書面或口頭的形式給出或 隱含，均將在本協議生效日期終止。除第 6.2～6.3 款列出的內容，基於您期望接受 此授權授權合約所做出的不實陳述(“誤解”)，您無須做出任何賠償；卡巴斯基實 驗室除依照此協議宣示的條款，也無須承擔任何責任。

8.2 本協議不能排除或限制卡巴斯基實驗室對任何已知不實的內容導致誤解的責任。

8.3 若對基本事項(包括供應商在本協議下履行其義務的能力)發生誤解，卡巴斯基實 驗室的責任按照第 6.3 款限定。對自願使用卡巴斯基實驗室的新版試用版產品的使用者，將無法享受本協定第 2 條中提供的技術支援服務。

8.4 如果您未遵守本《標準最終用戶授權授權合約》的條款，卡巴斯基實驗室有權 在不做任何通知的情況下終止授權。一旦發生此情況，您必須立即終止使用本軟體 並銷毀所有副本。